

SECURING AMERICA'S FEDERAL ELECTIONS ACT

—————  
JUNE 26, 2019.—Committed to the Committee of the Whole House on the State of  
the Union and ordered to be printed  
—————

Ms. LOFGREN, from the Committee of the Committee on House  
Administration, submitted the following

R E P O R T

together with

SUPPLEMENTAL VIEWS

[To accompany H.R. 2722]

[Including cost estimate of the Congressional Budget Office]

The Committee on House Administration, to whom was referred the bill (H.R. 2722) to protect elections for public office by providing financial support and enhanced security for the infrastructure used to carry out such elections, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

	Page
Amendment .....	2
Purpose and Summary .....	19
Background and Need for Legislation .....	20
Hearings .....	29
Committee Consideration .....	30
Committee Votes .....	30
Committee Oversight Findings .....	32
Statement of General Performance Goals and Objectives .....	32
New Budget Authority, Entitlement Authority, and Tax Expenditures .....	32
Earmarks and Tax and Tariff Benefits .....	32
Committee Cost Estimate .....	32
Congressional Budget Office Estimate .....	32
Federal Mandates Statement .....	35
Non-Duplication of Federal Programs .....	35
Advisory Committee Statement .....	35
Applicability to Legislative Branch .....	35
Section-by-Section Analysis of the Legislation .....	35

Changes in Existing Law Made by the Bill, as Reported .....	46
Supplemental Views .....	88

## AMENDMENT

The amendment is as follows:

Strike all after the enacting clause and insert the following:

### SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) **SHORT TITLE.**—This Act may be cited as the “Securing America’s Federal Elections Act” or the “SAFE Act”.

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

Sec. 1. Short title; table of contents.

#### TITLE I—FINANCIAL SUPPORT FOR ELECTION INFRASTRUCTURE

##### Subtitle A—Voting System Security Improvement Grants

#### PART 1—PROMOTING ACCURACY, INTEGRITY, AND SECURITY THROUGH VOTER-VERIFIED PERMANENT PAPER BALLOT

Sec. 101. Short title.

Sec. 102. Paper ballot and manual counting requirements.

Sec. 103. Accessibility and ballot verification for individuals with disabilities.

Sec. 104. Durability and readability requirements for ballots.

Sec. 105. Paper ballot printing requirements.

Sec. 106. Study and report on optimal ballot design.

Sec. 107. Effective date for new requirements.

#### PART 2—GRANTS TO CARRY OUT IMPROVEMENTS

Sec. 111. Grants for obtaining compliant paper ballot voting systems and carrying out voting system security improvements.

Sec. 112. Coordination of voting system security activities with use of requirements payments and election administration requirements under Help America Vote Act of 2002.

Sec. 113. Incorporation of definitions.

##### Subtitle B—Risk-Limiting Audits

Sec. 121. Risk-limiting audits.

Sec. 122. Funding for conducting post-election risk-limiting audits.

Sec. 123. GAO analysis of effects of audits.

#### TITLE II—PROMOTING CYBERSECURITY THROUGH IMPROVEMENTS IN ELECTION ADMINISTRATION

Sec. 201. Voting system cybersecurity requirements.

Sec. 202. Testing of existing voting systems to ensure compliance with election cybersecurity guidelines and other guidelines.

Sec. 203. Requiring use of software and hardware for which information is disclosed by manufacturer.

Sec. 204. Treatment of electronic poll books as part of voting systems.

Sec. 205. Pre-election reports on voting system usage.

Sec. 206. Streamlining collection of election information.

#### TITLE III—USE OF VOTING MACHINES MANUFACTURED IN THE UNITED STATES

Sec. 301. Use of voting machines manufactured in the United States.

#### TITLE IV—SEVERABILITY

Sec. 401. Severability.

## TITLE I—FINANCIAL SUPPORT FOR ELECTION INFRASTRUCTURE

### Subtitle A—Voting System Security Improvement Grants

#### PART 1—PROMOTING ACCURACY, INTEGRITY, AND SECURITY THROUGH VOTER-VERIFIED PERMANENT PAPER BALLOT

##### SEC. 101. SHORT TITLE.

This subtitle may be cited as the “Voter Confidence and Increased Accessibility Act of 2019”.

##### SEC. 102. PAPER BALLOT AND MANUAL COUNTING REQUIREMENTS.

(a) **IN GENERAL.**—Section 301(a)(2) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)(2)) is amended to read as follows:

“(2) PAPER BALLOT REQUIREMENT.—

“(A) VOTER-VERIFIED PAPER BALLOTS.—

“(i) PAPER BALLOT REQUIREMENT.—(I) The voting system shall require the use of an individual, durable, voter-verified paper ballot of the voter’s vote that shall be marked and made available for inspection and verification by the voter before the voter’s vote is cast and counted, and which shall be counted by hand or read by an optical character recognition device or other counting device. For purposes of this subclause, the term ‘individual, durable, voter-verified paper ballot’ means a paper ballot marked by the voter by hand or a paper ballot marked through the use of a nontabulating ballot marking device or system, so long as the voter shall have the option to mark his or her ballot by hand.

“(II) The voting system shall provide the voter with an opportunity to correct any error on the paper ballot before the permanent voter-verified paper ballot is preserved in accordance with clause (ii).

“(III) The voting system shall not preserve the voter-verified paper ballots in any manner that makes it possible, at any time after the ballot has been cast, to associate a voter with the record of the voter’s vote without the voter’s consent.

“(ii) PRESERVATION AS OFFICIAL RECORD.—The individual, durable, voter-verified paper ballot used in accordance with clause (i) shall constitute the official ballot and shall be preserved and used as the official ballot for purposes of any recount or audit conducted with respect to any election for Federal office in which the voting system is used.

“(iii) MANUAL COUNTING REQUIREMENTS FOR RECOUNTS AND AUDITS.—(I) Each paper ballot used pursuant to clause (i) shall be suitable for a manual audit, and shall be counted by hand in any recount or audit conducted with respect to any election for Federal office.

“(II) In the event of any inconsistencies or irregularities between any electronic vote tallies and the vote tallies determined by counting by hand the individual, durable, voter-verified paper ballots used pursuant to clause (i), and subject to subparagraph (B), the individual, durable, voter-verified paper ballots shall be the true and correct record of the votes cast.

“(iv) APPLICATION TO ALL BALLOTS.—The requirements of this subparagraph shall apply to all ballots cast in elections for Federal office, including ballots cast by absent uniformed services voters and overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act and other absentee voters.

“(B) SPECIAL RULE FOR TREATMENT OF DISPUTES WHEN PAPER BALLOTS HAVE BEEN SHOWN TO BE COMPROMISED.—

“(i) IN GENERAL.—In the event that—

“(I) there is any inconsistency between any electronic vote tallies and the vote tallies determined by counting by hand the individual, durable, voter-verified paper ballots used pursuant to subparagraph (A)(i) with respect to any election for Federal office; and

“(II) it is demonstrated by clear and convincing evidence (as determined in accordance with the applicable standards in the jurisdiction involved) in any recount, audit, or contest of the result of the election that the paper ballots have been compromised (by damage or mischief or otherwise) and that a sufficient number of the ballots have been so compromised that the result of the election could be changed,

the determination of the appropriate remedy with respect to the election shall be made in accordance with applicable State law, except that the electronic tally shall not be used as the exclusive basis for determining the official certified result.

“(ii) RULE FOR CONSIDERATION OF BALLOTS ASSOCIATED WITH EACH VOTING MACHINE.—For purposes of clause (i), only the paper ballots deemed compromised, if any, shall be considered in the calculation of whether or not the result of the election could be changed due to the compromised paper ballots.”

(b) CONFORMING AMENDMENT CLARIFYING APPLICABILITY OF ALTERNATIVE LANGUAGE ACCESSIBILITY.—Section 301(a)(4) of such Act (52 U.S.C. 21081(a)(4)) is amended by inserting “(including the paper ballots required to be used under paragraph (2))” after “voting system”.

(c) OTHER CONFORMING AMENDMENTS.—Section 301(a)(1) of such Act (52 U.S.C. 21081(a)(1)) is amended—

- (1) in subparagraph (A)(i), by striking “counted” and inserting “counted, in accordance with paragraphs (2) and (3)”;
- (2) in subparagraph (A)(ii), by striking “counted” and inserting “counted, in accordance with paragraphs (2) and (3)”;
- (3) in subparagraph (A)(iii), by striking “counted” each place it appears and inserting “counted, in accordance with paragraphs (2) and (3)”;
- (4) in subparagraph (B)(ii), by striking “counted” and inserting “counted, in accordance with paragraphs (2) and (3)”.

**SEC. 103. ACCESSIBILITY AND BALLOT VERIFICATION FOR INDIVIDUALS WITH DISABILITIES.**

**(a) BALLOT CYBERSECURITY, CONFIDENTIALITY, AND ACCESS FOR INDIVIDUALS WITH DISABILITIES.—**

(1) **IN GENERAL.**—Section 301(a)(3)(B) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)(3)(B)) is amended to read as follows:

“(B)(i) satisfy the requirement of subparagraph (A) through the use of at least 1 voting system at each polling place that—

“(I) is equipped for individuals with disabilities, including nonvisual and enhanced visual accessibility for the blind and visually impaired, and contains features to support enhanced manual accessibility for the mobility and dexterity impaired;

“(II) in the case of any election for Federal office occurring after the date that is 6 years after the date of the enactment of the Securing America’s Federal Elections Act—

“(aa) marks ballots that are identical in size, ink, and paper stock to those ballots that would be marked by hand or a ballot marking device used by voters who do not have accessibility needs;

“(bb) marks the ballot in such a way that someone examining the ballot will not be able to readily determine whether the ballot was marked by hand or machine; and

“(cc) combines ballots produced by the voting system with ballots marked by voters using other types of voting systems used by the State or jurisdiction in a way that prevents identification of which ballots were cast using each voting system; and

“(III) is made available for use by any voter who requests to use it; and

“(ii) in the case of any election for Federal office occurring after the date that is 6 years after the date of the enactment of the Securing America’s Federal Elections Act, meet the requirements of subparagraph (A) and paragraph (2)(A) by using a system that allows the voter to privately and independently verify the accuracy of the permanent paper ballot through the presentation, in accessible form, of the printed or marked vote selections from the same printed or marked information that would be used for any vote tabulation or auditing; and”.

(2) **CLARIFICATION WITH RESPECT TO APPLICATION OF REQUIREMENT TO BALLOTS MARKED AT HOME.**—Section 301(a)(3) of such Act (52 U.S.C. 21081(a)(3)) is amended by adding at the end the following new flush sentence:

“Nothing in subparagraph (B) shall be construed to prohibit the use of an accessible ballot that may be printed or marked by the voter at home.”.

**(b) SPECIFIC REQUIREMENT OF STUDY, TESTING, AND DEVELOPMENT OF ACCESSIBLE PAPER BALLOT VERIFICATION MECHANISMS.—**

(1) **STUDY AND REPORTING.**—Subtitle C of title II of such Act (52 U.S.C. 21081 et seq.) is amended—

(A) by redesignating section 247 as section 248; and

(B) by inserting after section 246 the following new section:

**“SEC. 247. STUDY AND REPORT ON ACCESSIBLE PAPER BALLOT VERIFICATION MECHANISMS.**

“(a) **STUDY AND REPORT.**—The Director of the National Science Foundation shall make grants to not fewer than 3 eligible entities to study, test, and develop accessible paper ballot voting, verification, and casting mechanisms and devices and best practices to enhance the accessibility of paper ballot voting and verification mechanisms for individuals with disabilities, for voters whose primary language is not English, and for voters with difficulties in literacy, including best practices for the mechanisms themselves and the processes through which the mechanisms are used.

“(b) **ELIGIBILITY.**—An entity is eligible to receive a grant under this part if it submits to the Director (at such time and in such form as the Director may require) an application containing—

“(1) certifications that the entity shall specifically investigate enhanced methods or devices, including non-electronic devices, that will assist such individuals and voters in marking voter-verified paper ballots and presenting or transmit-

ting the information printed or marked on such ballots back to such individuals and voters, and casting such ballots;

“(2) a certification that the entity shall complete the activities carried out with the grant not later than December 31, 2020; and

“(3) such other information and certifications as the Director may require.

“(c) AVAILABILITY OF TECHNOLOGY.—Any technology developed with the grants made under this section shall be treated as non-proprietary and shall be made available to the public, including to manufacturers of voting systems.

“(d) COORDINATION WITH GRANTS FOR TECHNOLOGY IMPROVEMENTS.—The Director shall carry out this section so that the activities carried out with the grants made under subsection (a) are coordinated with the research conducted under the grant program carried out by the Commission under section 271, to the extent that the Director and Commission determine necessary to provide for the advancement of accessible voting technology.

“(e) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out subsection (a) \$5,000,000, to remain available until expended.”.

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended—  
(A) by redesignating the item relating to section 247 as relating to section 248; and

(B) by inserting after the item relating to section 246 the following new item:

“Sec. 247. Study and report on accessible paper ballot verification mechanisms.”.

(c) CLARIFICATION OF ACCESSIBILITY STANDARDS UNDER VOLUNTARY VOTING SYSTEM GUIDANCE.—In adopting any voluntary guidance under subtitle B of title III of the Help America Vote Act with respect to the accessibility of the paper ballot verification requirements for individuals with disabilities, the Election Assistance Commission shall include and apply the same accessibility standards applicable under the voluntary guidance adopted for accessible voting systems under such subtitle.

(d) PERMITTING USE OF FUNDS FOR PROTECTION AND ADVOCACY SYSTEMS TO SUPPORT ACTIONS TO ENFORCE ELECTION-RELATED DISABILITY ACCESS.—Section 292(a) of the Help America Vote Act of 2002 (52 U.S.C. 21062(a)) is amended by striking “; except that” and all that follows and inserting a period.

#### SEC. 104. DURABILITY AND READABILITY REQUIREMENTS FOR BALLOTS.

Section 301(a) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)) is amended by adding at the end the following new paragraph:

“(7) DURABILITY AND READABILITY REQUIREMENTS FOR BALLOTS.—

“(A) DURABILITY REQUIREMENTS FOR PAPER BALLOTS.—

“(i) IN GENERAL.—All voter-verified paper ballots required to be used under this Act shall be marked or printed on durable paper.

“(ii) DEFINITION.—For purposes of this Act, paper is ‘durable’ if it is capable of withstanding multiple counts and recounts by hand without compromising the fundamental integrity of the ballots, and capable of retaining the information marked or printed on them for the full duration of a retention and preservation period of 22 months.

“(B) READABILITY REQUIREMENTS FOR PAPER BALLOTS MARKED BY BALLOT MARKING DEVICE.—All voter-verified paper ballots completed by the voter through the use of a ballot marking device shall be clearly readable by the voter without assistance (other than eyeglasses or other personal vision enhancing devices) and by an optical character recognition device or other device equipped for individuals with disabilities.”.

#### SEC. 105. PAPER BALLOT PRINTING REQUIREMENTS.

(a) REQUIRING PAPER BALLOTS TO BE PRINTED ON RECYCLED PAPER MANUFACTURED IN UNITED STATES.—Section 301(a) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)), as amended by section 104, is amended by adding at the end the following new paragraph:

“(8) PRINTING REQUIREMENTS FOR BALLOTS.—All paper ballots used in an election for Federal office shall be printed in the United States on recycled paper manufactured in the United States.”.

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall apply with respect to elections occurring on or after January 1, 2021.

#### SEC. 106. STUDY AND REPORT ON OPTIMAL BALLOT DESIGN.

(a) STUDY.—The Election Assistance Commission shall conduct a study of the best ways to design ballots used in elections for public office, including paper ballots and electronic or digital ballots, to minimize confusion and user errors.

(b) REPORT.—Not later than January 1, 2020, the Election Assistance Commission shall submit to Congress a report on the study conducted under subsection (a).

**SEC. 107. EFFECTIVE DATE FOR NEW REQUIREMENTS.**

Section 301(d) of the Help America Vote Act of 2002 (52 U.S.C. 21081(d)) is amended to read as follows:

“(d) EFFECTIVE DATE.—

“(1) IN GENERAL.—Except as provided in paragraph (2), each State and jurisdiction shall be required to comply with the requirements of this section on and after January 1, 2006.

“(2) SPECIAL RULE FOR CERTAIN REQUIREMENTS.—

“(A) IN GENERAL.—Except as provided in section 105(b) of the Securing America’s Federal Elections Act and subparagraphs (B) and (C), the requirements of this section which are first imposed on a State and jurisdiction pursuant to the amendments made by the Voter Confidence and Increased Accessibility Act of 2019 shall apply with respect to voting systems used for any election for Federal office held in 2020 or any succeeding year.

“(B) DELAY FOR JURISDICTIONS USING CERTAIN PAPER RECORD PRINTERS OR CERTAIN SYSTEMS USING OR PRODUCING VOTER-VERIFIED PAPER RECORDS IN 2018.—

“(i) DELAY.—In the case of a jurisdiction described in clause (ii), subparagraph (A) shall apply to a voting system in the jurisdiction as if the reference in such subparagraph to ‘2020’ were a reference to ‘2022’, but only with respect to the following requirements of this section:

“(I) Paragraph (2)(A)(i)(I) of subsection (a) (relating to the use of voter-verified paper ballots).

“(II) Paragraph (3)(B)(ii)(I) and (II) of subsection (a) (relating to access to verification from and casting of the durable paper ballot).

“(III) Paragraph (7) of subsection (a) (relating to durability and readability requirements for ballots).

“(ii) JURISDICTIONS DESCRIBED.—A jurisdiction described in this clause is a jurisdiction—

“(I) which used voter-verified paper record printers attached to direct recording electronic voting machines, or which used other voting systems that used or produced paper records of the vote verifiable by voters but that are not in compliance with paragraphs (2)(A)(i)(I), (3)(B)(iii)(I) and (II), and (7) of subsection (a) (as amended or added by the Voter Confidence and Increased Accessibility Act of 2019), for the administration of the regularly scheduled general election for Federal office held in November 2018; and

“(II) which will continue to use such printers or systems for the administration of elections for Federal office held in years before 2022.

“(iii) MANDATORY AVAILABILITY OF PAPER BALLOTS AT POLLING PLACES USING GRANDFATHERED PRINTERS AND SYSTEMS.—

“(I) REQUIRING BALLOTS TO BE OFFERED AND PROVIDED.—The appropriate election official at each polling place that uses a printer or system described in clause (ii)(I) for the administration of elections for Federal office shall offer each individual who is eligible to cast a vote in the election at the polling place the opportunity to cast the vote using a blank pre-printed paper ballot which the individual may mark by hand and which is not produced by the direct recording electronic voting machine or other such system. The official shall provide the individual with the ballot and the supplies necessary to mark the ballot, and shall ensure (to the greatest extent practicable) that the waiting period for the individual to cast a vote is the lesser of 30 minutes or the average waiting period for an individual who does not agree to cast the vote using such a paper ballot under this clause.

“(II) TREATMENT OF BALLOT.—Any paper ballot which is cast by an individual under this clause shall be counted and otherwise treated as a regular ballot for all purposes (including by incorporating it into the final unofficial vote count (as defined by the State) for the precinct) and not as a provisional ballot, unless the individual casting the ballot would have otherwise been required to cast a provisional ballot.

“(III) POSTING OF NOTICE.—The appropriate election official shall ensure there is prominently displayed at each polling place a notice

that describes the obligation of the official to offer individuals the opportunity to cast votes using a pre-printed blank paper ballot.

“(IV) TRAINING OF ELECTION OFFICIALS.—The chief State election official shall ensure that election officials at polling places in the State are aware of the requirements of this clause, including the requirement to display a notice under subclause (III), and are aware that it is a violation of the requirements of this title for an election official to fail to offer an individual the opportunity to cast a vote using a blank pre-printed paper ballot.

“(V) PERIOD OF APPLICABILITY.—The requirements of this clause apply only during the period in which the delay is in effect under clause (i).

“(C) SPECIAL RULE FOR JURISDICTIONS USING CERTAIN NONTABULATING BALLOT MARKING DEVICES.—In the case of a jurisdiction which uses a non-tabulating ballot marking device which automatically deposits the ballot into a privacy sleeve, subparagraph (A) shall apply to a voting system in the jurisdiction as if the reference in such subparagraph to ‘any election for Federal office held in 2020 or any succeeding year’ were a reference to ‘elections for Federal office occurring held in 2022 or each succeeding year’, but only with respect to paragraph (3)(B)(iii)(II) of subsection (a) (relating to nonmanual casting of the durable paper ballot).”.

## **PART 2—GRANTS TO CARRY OUT IMPROVEMENTS**

### **SEC. 111. GRANTS FOR OBTAINING COMPLIANT PAPER BALLOT VOTING SYSTEMS AND CARRYING OUT VOTING SYSTEM SECURITY IMPROVEMENTS.**

(a) AVAILABILITY OF GRANTS.—Subtitle D of title II of the Help America Vote Act of 2002 (52 U.S.C. 21001 et seq.) is amended by adding at the end the following new part:

#### **“PART 7—GRANTS FOR OBTAINING COMPLIANT PAPER BALLOT VOTING SYSTEMS AND CARRYING OUT VOTING SYSTEM SECURITY IMPROVEMENTS**

##### **“SEC. 297. GRANTS FOR OBTAINING COMPLIANT PAPER BALLOT VOTING SYSTEMS AND CARRYING OUT VOTING SYSTEM SECURITY IMPROVEMENTS.**

“(a) AVAILABILITY AND USE OF GRANT.—The Commission shall make a grant to each eligible State—

“(1) to replace a voting system—

“(A) which does not meet the requirements which are first imposed on the State pursuant to the amendments made by the Voter Confidence and Increased Accessibility Act of 2019 with a voting system which does meet such requirements, for use in the regularly scheduled general elections for Federal office held in November 2020, or

“(B) which does meet such requirements but which is not in compliance with the most recent voluntary voting system guidelines issued by the Commission prior to the regularly scheduled general election for Federal office held in November 2020 with another system which does meet such requirements and is in compliance with such guidelines;

“(2) to carry out voting system security improvements described in section 297A with respect to the regularly scheduled general elections for Federal office held in November 2020 and each succeeding election for Federal office; and

“(3) to implement and model best practices for ballot design, ballot instructions, and the testing of ballots.

“(b) AMOUNT OF GRANT.—The amount of a grant made to a State under this section shall be such amount as the Commission determines to be appropriate, except that such amount may not be less than the product of \$1 and the average of the number of individuals who cast votes in any of the two most recent regularly scheduled general elections for Federal office held in the State.

“(c) PRO RATA REDUCTIONS.—If the amount of funds appropriated for grants under this part is insufficient to ensure that each State receives the amount of the grant calculated under subsection (b), the Commission shall make such pro rata reductions in such amounts as may be necessary to ensure that the entire amount appropriated under this part is distributed to the States.

“(d) SURPLUS APPROPRIATIONS.—If the amount of funds appropriated for grants authorized under section 297D(a)(2) exceed the amount necessary to meet the re-

quirements of subsection (b), the Commission shall consider the following in making a determination to award remaining funds to a State:

“(1) The record of the State in carrying out the following with respect to the administration of elections for Federal office:

“(A) Providing voting machines that are less than 10 years old.

“(B) Implementing strong chain of custody procedures for the physical security of voting equipment and paper records at all stages of the process.

“(C) Conducting pre-election testing on every voting machine and ensuring that paper ballots are available wherever electronic machines are used.

“(D) Maintaining offline backups of voter registration lists.

“(E) Providing a secure voter registration database that logs requests submitted to the database.

“(F) Publishing and enforcing a policy detailing use limitations and security safeguards to protect the personal information of voters in the voter registration process.

“(G) Providing secure processes and procedures for reporting vote tallies.

“(H) Providing a secure platform for disseminating vote totals.

“(2) Evidence of established conditions of innovation and reform in providing voting system security and the proposed plan of the State for implementing additional conditions.

“(3) Evidence of collaboration between relevant stakeholders, including local election officials, in developing the grant implementation plan described in section 297B.

“(4) The plan of the State to conduct a rigorous evaluation of the effectiveness of the activities carried out with the grant.

“(e) ABILITY OF REPLACEMENT SYSTEMS TO ADMINISTER RANKED CHOICE ELECTIONS.—To the greatest extent practicable, an eligible State which receives a grant to replace a voting system under this section shall ensure that the replacement system is capable of administering a system of ranked choice voting under which each voter shall rank the candidates for the office in the order of the voter’s preference.

**“SEC. 297A. VOTING SYSTEM SECURITY IMPROVEMENTS DESCRIBED.**

“(a) PERMITTED USES.—A voting system security improvement described in this section is any of the following:

“(1) The acquisition of goods and services from qualified election infrastructure vendors by purchase, lease, or such other arrangements as may be appropriate.

“(2) Cyber and risk mitigation training.

“(3) A security risk and vulnerability assessment of the State’s election infrastructure which is carried out by a provider of cybersecurity services under a contract entered into between the chief State election official and the provider.

“(4) The maintenance of election infrastructure, including addressing risks and vulnerabilities which are identified under either of the security risk and vulnerability assessments described in paragraph (3), except that none of the funds provided under this part may be used to renovate or replace a building or facility which is used primarily for purposes other than the administration of elections for public office.

“(5) Providing increased technical support for any information technology infrastructure that the chief State election official deems to be part of the State’s election infrastructure or designates as critical to the operation of the State’s election infrastructure.

“(6) Enhancing the cybersecurity and operations of the information technology infrastructure described in paragraph (4).

“(7) Enhancing the cybersecurity of voter registration systems.

“(b) QUALIFIED ELECTION INFRASTRUCTURE VENDORS DESCRIBED.—

“(1) IN GENERAL.—For purposes of this part, a ‘qualified election infrastructure vendor’ is any person who provides, supports, or maintains, or who seeks to provide, support, or maintain, election infrastructure on behalf of a State, unit of local government, or election agency, who meets the criteria described in paragraph (2).

“(2) CRITERIA.—The criteria described in this paragraph are such criteria as the Chairman, in coordination with the Secretary of Homeland Security, shall establish and publish, and shall include each of the following requirements:

“(A) The vendor must be owned and controlled by a citizen or permanent resident of the United States.

“(B) The vendor must disclose to the Chairman and the Secretary, and to the chief State election official of any State to which the vendor provides any goods and services with funds provided under this part, of any sourcing outside the United States for parts of the election infrastructure.

“(C) The vendor agrees to ensure that the election infrastructure will be developed and maintained in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee.

“(D) The vendor agrees to maintain its information technology infrastructure in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee.

“(E) The vendor agrees to meet the requirements of paragraph (3) with respect to any known or suspected cybersecurity incidents involving any of the goods and services provided by the vendor pursuant to a grant under this part.

“(F) The vendor agrees to permit independent security testing by the Commission (in accordance with section 231(a)) and by the Secretary of the goods and services provided by the vendor pursuant to a grant under this part.

“(3) CYBERSECURITY INCIDENT REPORTING REQUIREMENTS.—

“(A) IN GENERAL.—A vendor meets the requirements of this paragraph if, upon becoming aware of the possibility that an election cybersecurity incident has occurred involving any of the goods and services provided by the vendor pursuant to a grant under this part—

“(i) the vendor promptly assesses whether or not such an incident occurred, and submits a notification meeting the requirements of subparagraph (B) to the Secretary and the Chairman of the assessment as soon as practicable (but in no case later than 3 days after the vendor first becomes aware of the possibility that the incident occurred);

“(ii) if the incident involves goods or services provided to an election agency, the vendor submits a notification meeting the requirements of subparagraph (B) to the agency as soon as practicable (but in no case later than 3 days after the vendor first becomes aware of the possibility that the incident occurred), and cooperates with the agency in providing any other necessary notifications relating to the incident; and

“(iii) the vendor provides all necessary updates to any notification submitted under clause (i) or clause (ii).

“(B) CONTENTS OF NOTIFICATIONS.—Each notification submitted under clause (i) or clause (ii) of subparagraph (A) shall contain the following information with respect to any election cybersecurity incident covered by the notification:

“(i) The date, time, and time zone when the election cybersecurity incident began, if known.

“(ii) The date, time, and time zone when the election cybersecurity incident was detected.

“(iii) The date, time, and duration of the election cybersecurity incident.

“(iv) The circumstances of the election cybersecurity incident, including the specific election infrastructure systems believed to have been accessed and information acquired, if any.

“(v) Any planned and implemented technical measures to respond to and recover from the incident.

“(vi) In the case of any notification which is an update to a prior notification, any additional material information relating to the incident, including technical data, as it becomes available.

“SEC. 297B. ELIGIBILITY OF STATES.

“A State is eligible to receive a grant under this part if the State submits to the Commission, at such time and in such form as the Commission may require, an application containing—

“(1) a description of how the State will use the grant to carry out the activities authorized under this part;

“(2) a certification and assurance that, not later than 5 years after receiving the grant, the State will carry out voting system security improvements, as described in section 297A; and

“(3) such other information and assurances as the Commission may require.

“SEC. 297C. REPORTS TO CONGRESS.

“Not later than 90 days after the end of each fiscal year, the Commission shall submit a report to the appropriate congressional committees, including the Committees on Homeland Security, House Administration, and the Judiciary of the House of Representatives and the Committees on Homeland Security and Governmental Affairs, the Judiciary, and Rules and Administration of the Senate, on the activities carried out with the funds provided under this part.

**“SEC. 297D. AUTHORIZATION OF APPROPRIATIONS.**

“(a) AUTHORIZATION.—There are authorized to be appropriated for grants under this part—

- “(1) \$600,000,000 for fiscal year 2019; and
- “(2) \$175,000,000 for each of the fiscal years 2020, 2022, 2024, and 2026.

“(b) CONTINUING AVAILABILITY OF AMOUNTS.—Any amounts appropriated pursuant to the authorization of this section shall remain available until expended.”.

(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—GRANTS FOR OBTAINING COMPLIANT PAPER BALLOT VOTING SYSTEMS AND CARRYING OUT VOTING SYSTEM SECURITY IMPROVEMENTS

“Sec. 297. Grants for obtaining compliant paper ballot voting systems and carrying out voting system security improvements.

“Sec. 297A. Voting system security improvements described.

“Sec. 297B. Eligibility of States.

“Sec. 297C. Reports to Congress.

“Sec. 297D. Authorization of appropriations.”.

**SEC. 112. COORDINATION OF VOTING SYSTEM SECURITY ACTIVITIES WITH USE OF REQUIREMENTS PAYMENTS AND ELECTION ADMINISTRATION REQUIREMENTS UNDER HELP AMERICA VOTE ACT OF 2002.**

(a) DUTIES OF ELECTION ASSISTANCE COMMISSION.—Section 202 of the Help America Vote Act of 2002 (52 U.S.C. 20922) is amended in the matter preceding paragraph (1) by striking “by” and inserting “and the security of election infrastructure by”.

(b) MEMBERSHIP OF SECRETARY OF HOMELAND SECURITY ON BOARD OF ADVISORS OF ELECTION ASSISTANCE COMMISSION.—Section 214(a) of such Act (52 U.S.C. 20944(a)) is amended—

- (1) by striking “37 members” and inserting “38 members”; and
- (2) by adding at the end the following new paragraph:  
“(17) The Secretary of Homeland Security or the Secretary’s designee.”.

(c) REPRESENTATIVE OF DEPARTMENT OF HOMELAND SECURITY ON TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE.—Section 221(c)(1) of such Act (52 U.S.C. 20961(c)(1)) is amended—

- (1) by redesignating subparagraph (E) as subparagraph (F); and
- (2) by inserting after subparagraph (D) the following new subparagraph:  
“(E) A representative of the Department of Homeland Security.”.

(d) GOALS OF PERIODIC STUDIES OF ELECTION ADMINISTRATION ISSUES; CONSULTATION WITH SECRETARY OF HOMELAND SECURITY.—Section 241(a) of such Act (52 U.S.C. 20981(a)) is amended—

- (1) in the matter preceding paragraph (1), by striking “the Commission shall” and inserting “the Commission, in consultation with the Secretary of Homeland Security (as appropriate), shall”;
- (2) by striking “and” at the end of paragraph (3);
- (3) by redesignating paragraph (4) as paragraph (5); and
- (4) by inserting after paragraph (3) the following new paragraph:  
“(4) will be secure against attempts to undermine the integrity of election systems by cyber or other means; and”.

(e) REQUIREMENTS PAYMENTS.—

(1) USE OF PAYMENTS FOR VOTING SYSTEM SECURITY IMPROVEMENTS.—Section 251(b) of such Act (52 U.S.C. 21001(b)) is amended by adding at the end the following new paragraph:

“(4) PERMITTING USE OF PAYMENTS FOR VOTING SYSTEM SECURITY IMPROVEMENTS.—A State may use a requirements payment to carry out any of the following activities:

- “(A) Cyber and risk mitigation training.
- “(B) Providing increased technical support for any information technology infrastructure that the chief State election official deems to be part of the State’s election infrastructure or designates as critical to the operation of the State’s election infrastructure.
- “(C) Enhancing the cybersecurity and operations of the information technology infrastructure described in subparagraph (B).
- “(D) Enhancing the security of voter registration databases.”.

(2) INCORPORATION OF ELECTION INFRASTRUCTURE PROTECTION IN STATE PLANS FOR USE OF PAYMENTS.—Section 254(a)(1) of such Act (52 U.S.C. 21004(a)(1)) is amended by striking the period at the end and inserting “, including the protection of election infrastructure.”.

(3) COMPOSITION OF COMMITTEE RESPONSIBLE FOR DEVELOPING STATE PLAN FOR USE OF PAYMENTS.—Section 255 of such Act (52 U.S.C. 21005) is amended—

- (A) by redesignating subsection (b) as subsection (c); and
- (B) by inserting after subsection (a) the following new subsection:

“(b) GEOGRAPHIC REPRESENTATION.—The members of the committee shall be a representative group of individuals from the State’s counties, cities, towns, and Indian tribes, and shall represent the needs of rural as well as urban areas of the State, as the case may be.”

(f) ENSURING PROTECTION OF COMPUTERIZED STATEWIDE VOTER REGISTRATION LIST.—Section 303(a)(3) of such Act (52 U.S.C. 21083(a)(3)) is amended by striking the period at the end and inserting “, as well as other measures to prevent and deter cybersecurity incidents, as identified by the Commission, the Secretary of Homeland Security, and the Technical Guidelines Development Committee.”

**SEC. 113. INCORPORATION OF DEFINITIONS.**

(a) IN GENERAL.—Section 901 of the Help America Vote Act of 2002 (52 U.S.C. 21141) is amended to read as follows:

**“SEC. 901. DEFINITIONS.**

“In this Act, the following definitions apply:

“(1) The term ‘cybersecurity incident’ has the meaning given the term ‘incident’ in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148).

“(2) The term ‘election agency’ means any component of a State, or any component of a unit of local government in a State, which is responsible for the administration of elections for Federal office in the State.

“(3) The term ‘election infrastructure’ means storage facilities, polling places, and centralized vote tabulation locations used to support the administration of elections for public office, as well as related information and communications technology, including voter registration databases, voting machines, 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 other systems used to manage the election process and to report and display election results on behalf of an election agency.

“(4) The term ‘State’ means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the United States Virgin Islands, and the Commonwealth of the Northern Mariana Islands.”

(b) CLERICAL AMENDMENT.—The table of contents of such Act is amended by amending the item relating to section 901 to read as follows:

“Sec. 901. Definitions.”

## Subtitle B—Risk-Limiting Audits

**SEC. 121. RISK-LIMITING AUDITS.**

(a) IN GENERAL.— Title III of the Help America Vote Act of 2002 (52 U.S.C. 21081 et seq.) is amended by inserting after section 303 the following new section:

**“SEC. 303A. RISK-LIMITING AUDITS.**

“(a) DEFINITIONS.—In this section:

“(1) RISK-LIMITING AUDIT.—The term ‘risk-limiting audit’ means, with respect to any election contest, a post-election process that—

“(A) has a probability of at least 95 percent of correcting the reported outcome if the reported outcome is not the correct outcome;

“(B) will not change the outcome if the reported outcome is the correct outcome; and

“(C) involves a manual adjudication of voter intent from some or all of the ballots validly cast in the election contest.

“(2) REPORTED OUTCOME; CORRECT OUTCOME; OUTCOME.—

“(A) REPORTED OUTCOME.—The term ‘reported outcome’ means the outcome of an election contest which is determined according to the canvass and which will become the official, certified outcome unless it is revised by an audit, recount, or other legal process.

“(B) CORRECT OUTCOME.—The term ‘correct outcome’ means the outcome that would be determined by a manual adjudication of voter intent for all votes validly cast in the election contest.

“(C) OUTCOME.—The term ‘outcome’ means the winner or set of winners of an election contest.

“(3) MANUAL ADJUDICATION OF VOTER INTENT.—The term ‘manual adjudication of voter intent’ means direct inspection and determination by humans,

without assistance from electronic or mechanical tabulation devices, of the ballot choices marked by voters on each voter-verified paper record.

“(4) BALLOT MANIFEST.—The term ‘ballot manifest’ means a record maintained by each jurisdiction that—

“(A) is created without reliance on any part of the voting system used to tabulate votes;

“(B) functions as a sampling frame for conducting a risk-limiting audit; and

“(C) accounts for all ballots validly cast regardless of how or whether they were tabulated and includes a precise description of the manner in which the ballots are physically stored, including the total number of physical groups of ballots, the numbering system for each group, a unique label for each group, and the number of ballots in each such group.

“(b) REQUIREMENTS.—

“(1) IN GENERAL.—

“(A) AUDITS.—

“(i) IN GENERAL.—Each State and jurisdiction shall administer risk-limiting audits of the results of all election contests for Federal office held in the State in accordance with the requirements of paragraph (2).

“(ii) EXCEPTION.—Clause (i) shall not apply to any election contest for which the State or jurisdiction conducts a full recount through a manual adjudication of voter intent.

“(B) FULL MANUAL TABULATION.—If a risk-limiting audit conducted under subparagraph (A) corrects the reported outcome of an election contest, the State or jurisdiction shall use the results of the manual adjudication of voter intent conducted as part of the risk-limiting audit as the official results of the election contest.

“(2) AUDIT REQUIREMENTS.—

“(A) RULES AND PROCEDURES.—

“(i) IN GENERAL.—Not later than 1 year after the date of the enactment of this section, the chief State election official of the State shall establish rules and procedures for conducting risk-limiting audits.

“(ii) MATTERS INCLUDED.—The rules and procedures established under clause (i) shall include the following:

“(I) Rules and procedures for ensuring the security of ballots and documenting that prescribed procedures were followed.

“(II) Rules and procedures for ensuring the accuracy of ballot manifests produced by jurisdictions.

“(III) Rules and procedures for governing the format of ballot manifests and other data involved in risk-limiting audits.

“(IV) Methods to ensure that any cast vote records used in a risk-limiting audit are those used by the voting system to tally the results of the election contest sent to the chief State election official of the State and made public.

“(V) Rules and procedures for the random selection of ballots to be inspected manually during each audit.

“(VI) Rules and procedures for the calculations and other methods to be used in the audit and to determine whether and when the audit of each election contest is complete.

“(VII) Rules and procedures for testing any software used to conduct risk-limiting audits.

“(B) PUBLIC REPORT.—

“(i) IN GENERAL.—After the completion of the risk-limiting audit and at least 5 days before the election contest is certified, the State shall publish a report on the results of the audit, together with such information as necessary to confirm that the audit was conducted properly.

“(ii) FORMAT OF DATA.—All data published with the report under clause (i) shall be published in machine-readable, open data formats.

“(iii) PROTECTION OF ANONYMITY OF VOTES.—Information and data published by the State under this subparagraph shall not compromise the anonymity of votes.

“(c) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this section for the first regularly scheduled election for Federal office held more than 1 year after the date of the enactment of the Securing America’s Federal Elections Act and for each subsequent election for Federal office.”.

(b) CONFORMING AMENDMENTS RELATED TO ENFORCEMENT.—Section 401 of such Act (52 U.S.C. 21111) is amended by striking “and 303” and inserting “303, and 303A”.

(c) CLERICAL AMENDMENT.—The table of contents for such Act is amended by inserting after the item relating to section 303 the following new item:

“Sec. 303A. Risk-limiting audits.”.

**SEC. 122. FUNDING FOR CONDUCTING POST-ELECTION RISK-LIMITING AUDITS.**

(a) PAYMENTS TO STATES.— Subtitle D of title II of the Help America Vote Act of 2002 (52 U.S.C. 21001 et seq.), as amended by section 111(a), is amended by adding at the end the following new part:

**“PART 8—FUNDING FOR POST-ELECTION RISK-LIMITING AUDITS**

**“SEC. 298. PAYMENTS FOR POST-ELECTION RISK-LIMITING AUDITS.**

“(a) IN GENERAL.—The Commission shall pay to States the amount of eligible post-election audit costs.

“(b) ELIGIBLE POST-ELECTION AUDIT COSTS.—For purposes of this section, the term ‘eligible post-election audit costs’ means, with respect to any State, costs paid or incurred by the State or local government within the State for—

“(1) the conduct of any risk-limiting audit (as defined in section 303A) with respect to an election for Federal office occurring after the date of the enactment of this part; and

“(2) any equipment, software, or services necessary for the conduct of any such risk-limiting audit.

“(c) SPECIAL RULES.—

“(1) RULES AND PROCEDURES.—The Commission shall establish rules and procedures for submission of eligible post-election audit costs for payments under this section.

“(2) INSUFFICIENT FUNDS.—In any case in which the amounts appropriated under subsection (d) are insufficient to pay all eligible post-election audit costs submitted by States with respect to any Federal election, the amount of such costs paid under subsection (a) to any State shall be equal to the amount that bears the same ratio to the amount which would be paid to such State (determined without regard to this paragraph) as—

“(A) the number of individuals who voted in such Federal election in such State; bears to

“(B) the total number of individuals who voted in such Federal election in all States submitting a claim for eligible post-election audit costs.

“(d) AUTHORIZATION OF APPROPRIATIONS.—

“(1) IN GENERAL.—There is hereby authorized to be appropriated to the Commission such sums as are necessary to carry out this part.

“(2) AVAILABILITY.—Any amounts appropriated pursuant to paragraph (1) shall remain available without fiscal year limitation until expended.”.

(b) CLERICAL AMENDMENT.—The table of contents of such Act, as amended by section 111(b), is further amended by adding at the end of the items relating to subtitle D of title II the following:

**“PART 8—FUNDING FOR POST-ELECTION RISK-LIMITING AUDITS**

“Sec. 298. Payments for post-election risk-limiting audits.”.

**SEC. 123. GAO ANALYSIS OF EFFECTS OF AUDITS.**

(a) ANALYSIS.—Not later than 6 months after the first elections for Federal office is held for which States must conduct risk-limiting audits under section 303A of the Help America Vote Act of 2002 (as added by section 121), the Comptroller General of the United States shall conduct an analysis of the extent to which such audits have improved the administration of such elections and the security of election infrastructure in the States receiving such grants.

(b) REPORT.—The Comptroller General of the United States shall submit a report on the analysis conducted under subsection (a) to the Committee on House Administration of the House of Representatives and the Committee on Rules and Administration of the Senate.

## TITLE II—PROMOTING CYBERSECURITY THROUGH IMPROVEMENTS IN ELECTION AD- MINISTRATION

### SEC. 201. VOTING SYSTEM CYBERSECURITY REQUIREMENTS.

(a) **BALLOT TABULATING DEVICES.**— Section 301(a) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)), as amended by section 104 and section 105, is further amended by adding at the end the following new paragraph:

“(9) **BALLOT TABULATING METHODS.**—

“(A) **IN GENERAL.**—The voting system tabulates ballots by hand or through the use of an optical scanning device that meets the requirements of subparagraph (B).

“(B) **REQUIREMENTS FOR OPTICAL SCANNING DEVICES.**—Except as provided in subparagraph (C), the requirements of this subparagraph are as follows:

“(i) The device is designed and built in a manner in which it is mechanically impossible for the device to add or change the vote selections on a printed or marked ballot.

“(ii) The device is capable of exporting its data (including vote tally data sets and cast vote records) in a machine-readable, open data standard format required by the Commission, in consultation with the Director of the National Institute of Standards and Technology.

“(iii) The device consists of hardware that—

“(I) is certified under section 2216 of the Homeland Security Act; and

“(II) demonstrably conforms to a hardware component manifest describing point-of-origin information (including upstream hardware supply chain information for each component) that—

“(aa) has been provided to the Commission, the Director of Cybersecurity and Infrastructure Security under section 2215 of the Homeland Security Act, and the chief State election official for each State in which the device is used; and

“(bb) may be shared by any entity to whom it has been provided under item (aa) with independent experts for cybersecurity analysis.

“(iv) The device utilizes technology that prevents the operation of the device if any hardware components do not meet the requirements of clause (iii).

“(v) The device operates using software—

“(I) for which the source code, system build tools, and compilation parameters—

“(aa) have been provided to the Commission, the Director of Cybersecurity and Infrastructure Security under section 2215 of the Homeland Security Act, and the chief State election official for each State in which the device is used; and

“(bb) may be shared by any entity to whom it has been provided under item (aa) with independent experts for cybersecurity analysis; and

“(II) that is certified under section 2216 of the Homeland Security Act.

“(vi) The device utilizes technology that prevents the running of software on the device that does not meet the requirements of clause (v).

“(vii) The device utilizes technology that enables election officials, cybersecurity researchers, and voters to verify that the software running on the device—

“(I) was built from a specific, untampered version of the code that is described in clause (v); and

“(II) uses the system build tools and compilation parameters that are described in clause (v).

“(viii) The device contains such other security requirements as the Director of Cybersecurity and Infrastructure Security requires.

“(C) **WAIVER.**—

“(i) **IN GENERAL.**—The Director of Cybersecurity and Infrastructure Security, in consultation with the Director of the National Institute of Standards and Technology, may waive one or more of the requirements of subparagraph (B) (other than the requirement of clause (i) thereof) with respect to any device for a period of not to exceed 2 years.

- “(ii) PUBLICATION.—Information relating to any waiver granted under clause (i) shall be made publicly available on the Internet.
- “(D) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this paragraph for the regularly scheduled election for Federal office in November 2024, and for each subsequent election for Federal office.”.
- (b) OTHER CYBERSECURITY REQUIREMENTS.— Section 301(a) of such Act (52 U.S.C. 21081(a)), as amended by section 104, section 105, and subsection (a), is further amended by adding at the end the following new paragraphs:
- “(10) PROHIBITION OF USE OF WIRELESS COMMUNICATIONS DEVICES IN SYSTEMS OR DEVICES.—
- “(A) IN GENERAL.—No system or device upon which ballot marking devices or optical scanners are configured, upon which ballots are marked by voters (except as necessary for individuals with disabilities to use ballot marking devices that meet the accessibility requirements of paragraph (3)), or upon which votes are cast, tabulated, or aggregated shall contain, use, or be accessible by any wireless, power-line, or concealed communication device.
- “(B) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this paragraph for the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office.
- “(11) PROHIBITING CONNECTION OF SYSTEM TO THE INTERNET.—
- “(A) IN GENERAL.—No system or device upon which ballot marking devices or optical scanners are configured, upon which ballots are marked by voters, or upon which votes are cast, tabulated, or aggregated shall be connected to the Internet or any non-local computer system via telephone or other communication network at any time.
- “(B) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this paragraph for the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office.”.
- (c) SPECIAL CYBERSECURITY RULES FOR CERTAIN BALLOT MARKING DEVICES.—
- (1) IN GENERAL.—Section 301(a) of such Act (52 U.S.C. 21081(a)), as amended by section 104, section 105, and subsections (a) and (b), is further amended by adding at the end the following new paragraph:
- “(13) BALLOT MARKING DEVICES.—
- “(A) IN GENERAL.—In the case of a voting system that uses a ballot marking device, the ballot marking device shall be a device that—
- “(i) is not capable of tabulating votes;
- “(ii) except in the case of a ballot marking device used exclusively to comply with the requirements of paragraph (3), is certified in accordance with section 232 as meeting the requirements of subparagraph (B); and
- “(iii) is certified under section 2216 of the Homeland Security Act as meeting the requirements of clauses (iii) through (viii) of section 301(a)(9)(B).
- “(B) REQUIREMENTS.—
- “(i) IN GENERAL.—A ballot marking device meets the requirements of this subparagraph if, during a double-masked test conducted by a qualified independent user experience research laboratory (as defined in section 232(b)(4)) of a simulated election scenario which meets the requirements of clause (ii), there is less than a 5 percent chance that an ordinary voter using the device would not detect and report any difference between the vote selection printed on the ballot by the ballot marking device and the vote selection indicated by the voter.
- “(ii) SIMULATED ELECTION SCENARIO.—A simulated election scenario meets the requirements of this clause if it is conducted with—
- “(I) a pool of subjects that are—
- “(aa) diverse in age, gender, education, and physical limitations; and
- “(bb) representative of the communities in which the voting system will be used; and
- “(II) ballots that are representative of ballots ordinarily used in the communities in which the voting system will be used.
- “(C) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this paragraph for the regularly scheduled election for Federal office in November 2022, and for each subsequent election for Federal office.”.

## (2) PROCEDURE FOR TESTING.—

(A) IN GENERAL.—Subtitle B of title II of the Help America Vote Act of 2002 (52 U.S.C. 20971 et seq.) is amended by adding at the end the following new section:

**“SEC. 232. TESTING AND CERTIFICATION OF BALLOT MARKING DEVICES.**

“(a) IN GENERAL.—Any State or jurisdiction which intends to use a ballot marking device (other than a ballot marking device used exclusively to comply with the requirements of section 301(a)(3)) in an election for Federal office may submit an application to the Commission for testing and certification under this section.

**“(b) APPLICATION, ASSIGNMENT, AND TESTING.—**

“(1) IN GENERAL.—An application under subsection (a) shall be submitted not later than 18 months before the date of the election for Federal office in which the ballot marking device is intended to be used and shall contain such information as the Commission requires.

“(2) ASSIGNMENT.—Upon receipt of an application for testing under this section, the Commission shall contract with a qualified independent user experience research laboratory for the testing of whether the ballot marking device intended to be used by the State or jurisdiction meets the requirements of section 301(a)(10)(B).

“(3) REQUIREMENTS FOR TESTING.—Any contract described in paragraph (2) shall require the qualified independent user experience research laboratory to—

“(A) not later than 30 days before testing begins, submit to the Commission for approval the protocol for the simulated election scenario used for testing the ballot marking device;

“(B) use only protocols approved by the Commission in conducting such testing; and

“(C) submit to the Commission a report on the results of the testing.

“(4) QUALIFIED INDEPENDENT USER EXPERIENCE RESEARCH LABORATORY.—For purposes of this section:

“(A) IN GENERAL.—The term ‘qualified independent user experience research laboratory’ means a laboratory accredited under this subsection by the Election Assistance Commission in accordance with standards determined by the Commission, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security.

“(B) CRITERIA.—A laboratory shall not be accredited under this subsection unless such laboratory demonstrates that—

“(i) no employee of, or individual with an ownership in, such laboratory has, or has had during the 5 preceding years, any financial relationship with a manufacturer of voting systems; and

“(ii) any group of individuals conducting tests under this section collectively meet the following qualifications:

“(I) Experience designing and running user research studies and experiments using both qualitative and quantitative methodologies.

“(II) Experience with voting systems.

**“(c) REVIEW BY INDEPENDENT BOARD.—**

“(1) IN GENERAL.—The Commission shall submit for approval to an independent review board established under paragraph (3) the following:

“(A) Any protocol submitted to the Commission under subsection (b)(3)(A).

“(B) Any report submitted to the Commission under subsection (b)(3)(C).

“(2) FINAL APPROVAL.—Not later than the date that is 12 months before the date of the election for Federal office in which a State or jurisdiction intends to use the ballot marking device, the independent review board shall report to the Commission on whether it has approved a report submitted under paragraph (1)(B).

**“(3) INDEPENDENT REVIEW BOARD.—**

“(A) IN GENERAL.—An independent review board established under this paragraph shall be composed of 5 independent scientists appointed by the Commission, in consultation with the Director of the National Institute of Standards and Technology.

“(B) QUALIFICATIONS.—The members of the independent review board—

“(i) shall have expertise and relevant peer-reviewed publications in the following fields: cognitive psychology, experimental design, statistics, and user experience research and testing; and

“(ii) may not have, or have had during the 5 preceding years, any financial relationship with a manufacturer of voting systems.

“(4) PUBLICATION.—The Commission shall make public—

“(A) any protocol approved under this subsection;

- “(B) any report submitted under subsection (b)(3)(C); and  
“(C) any determination made by an independent review board under paragraph (2).  
“(d) CERTIFICATION.—If—  
“(1) a ballot marking device is determined by the qualified independent user experience research laboratory to meet the requirements of section 301(a)(7); and  
“(2) the report submitted under subsection (b)(3)(C) is approved by a majority of the members of the independent review board under subsection (d)(2), then the Commission shall certify the ballot marking device.  
“(e) PROHIBITION ON FEES.—The Commission may not charge any fee to a State or jurisdiction, a developer or manufacturer of a ballot marking device, or any other person in connection with testing and certification under this section.”.
- (B) CONFORMING AMENDMENTS.—  
(i) Section 202(2) of the Help America Vote Act of 2002 (52 U.S.C. 20922(2)) is amended by inserting “and ballot marking devices” after “hardware and software”.  
(ii) The heading for subtitle B of title II of such Act is amended by inserting at the end “; **Ballot Marking Devices**”.  
(iii) The table of contents of such Act is amended—  
(I) by inserting “; Ballot Marking Devices” at the end of the item relating to subtitle B of title II; and  
(II) by inserting after the item related to section 231 the following:

“Sec. 232. Testing and certification of ballot marking devices.”.

**SEC. 202. TESTING OF EXISTING VOTING SYSTEMS TO ENSURE COMPLIANCE WITH ELECTION CYBERSECURITY GUIDELINES AND OTHER GUIDELINES.**

- (a) REQUIRING TESTING OF EXISTING VOTING SYSTEMS.—  
(1) IN GENERAL.—Section 231(a) of the Help America Vote Act of 2002 (52 U.S.C. 20971(a)) is amended by adding at the end the following new paragraph:  
“(3) TESTING TO ENSURE COMPLIANCE WITH GUIDELINES.—  
“(A) TESTING.—Not later than 9 months before the date of each regularly scheduled general election for Federal office, the Commission shall provide for the testing by accredited laboratories under this section of the voting system hardware and software which was certified for use in the most recent such election, on the basis of the most recent voting system guidelines applicable to such hardware or software (including election cybersecurity guidelines) issued under this Act.  
“(B) DECERTIFICATION OF HARDWARE OR SOFTWARE FAILING TO MEET GUIDELINES.—If, on the basis of the testing described in subparagraph (A), the Commission determines that any voting system hardware or software does not meet the most recent guidelines applicable to such hardware or software issued under this Act, the Commission shall decertify such hardware or software.”.  
(2) EFFECTIVE DATE.—The amendment made by paragraph (1) shall apply with respect to the regularly scheduled general election for Federal office held in November 2020 and each succeeding regularly scheduled general election for Federal office.  
(b) ISSUANCE OF CYBERSECURITY GUIDELINES BY TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE.—Section 221(b) of the Help America Vote Act of 2002 (52 U.S.C. 20961(b)) is amended by adding at the end the following new paragraph:  
“(3) ELECTION CYBERSECURITY GUIDELINES.—Not later than 6 months after the date of the enactment of the Securing America’s Federal Elections Act, the Development Committee shall issue election cybersecurity guidelines, including standards and best practices for procuring, maintaining, testing, operating, and updating election systems to prevent and deter cybersecurity incidents.”.

**SEC. 203. REQUIRING USE OF SOFTWARE AND HARDWARE FOR WHICH INFORMATION IS DISCLOSED BY MANUFACTURER.**

- (a) REQUIREMENT.—Section 301(a) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)), as amended by sections 104 and 105, is amended by adding at the end the following new paragraph:  
“(9) REQUIRING USE OF SOFTWARE AND HARDWARE FOR WHICH INFORMATION IS DISCLOSED BY MANUFACTURER.—  
“(A) REQUIRING USE OF SOFTWARE FOR WHICH SOURCE CODE IS DISCLOSED BY MANUFACTURER.—  
“(i) IN GENERAL.—In the operation of voting systems in an election for Federal office, a State may only use software for which the manufacturer makes the source code (in the form in which will be used at

the time of the election) publicly available online under a license that grants a worldwide, royalty-free, non-exclusive, perpetual, sub-licensable license to all intellectual property rights in such source code, except that the manufacturer may prohibit a person who obtains the software from using the software in a manner that is primarily intended for or directed toward commercial advantage or private monetary compensation that is unrelated to carrying out legitimate research or cybersecurity activity.

“(ii) EXCEPTIONS.—Clause (i) does not apply with respect to—

“(I) widely-used operating system software which is not specific to voting systems and for which the source code or baseline functionality is not altered; or

“(II) widely-used cybersecurity software which is not specific to voting systems and for which the source code or baseline functionality is not altered.

“(B) REQUIRING USE OF HARDWARE FOR WHICH INFORMATION IS DISCLOSED BY MANUFACTURER.—

“(i) REQUIRING DISCLOSURE OF HARDWARE.—A State may not use a voting system in an election for Federal office unless the manufacturer of the system publicly discloses online the identification of the hardware used to operate the system.

“(ii) ADDITIONAL DISCLOSURE REQUIREMENTS FOR CUSTOM OR ALTERED HARDWARE.—To the extent that the hardware used to operate a voting system or any component thereof is not widely-used, or is widely-used but is altered, the State may not use the system in an election for Federal office unless—

“(I) the manufacturer of the system publicly discloses online the components of the hardware, the design of such components, and how such components are connected in the operation of the system; and

“(II) the manufacturer makes the design (in the form which will be used at the time of the election) publicly available online under a license that grants a worldwide, royalty-free, non-exclusive, perpetual, sub-licensable license to all intellectual property rights in the design of the hardware or the component, except that the manufacturer may prohibit a person who obtains the design from using the design in a manner that is primarily intended for or directed toward commercial advantage or private monetary compensation that is unrelated to carrying out legitimate research or cybersecurity activity.”

(b) EFFECTIVE DATE.—The amendment made by subsection (a) shall apply with respect to elections for Federal office held in 2020 or any succeeding year.

**SEC. 204. TREATMENT OF ELECTRONIC POLL BOOKS AS PART OF VOTING SYSTEMS.**

(a) INCLUSION IN DEFINITION OF VOTING SYSTEM.—Section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b)) is amended—

(1) in the matter preceding paragraph (1), by striking “this section” and inserting “this Act”;

(2) by striking “and” at the end of paragraph (1);

(3) by redesignating paragraph (2) as paragraph (3); and

(4) by inserting after paragraph (1) the following new paragraph:

“(2) any electronic poll book used with respect to the election; and”.

(b) DEFINITION.—Section 301 of such Act (52 U.S.C. 21081) is amended—

(1) by redesignating subsections (c) and (d) as subsections (d) and (e); and

(2) by inserting after subsection (b) the following new subsection:

“(c) ELECTRONIC POLL BOOK DEFINED.—In this Act, the term ‘electronic poll book’ means the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—

“(1) to retain the list of registered voters at a polling location, or vote center, or other location at which voters cast votes in an election for Federal office; and

“(2) to identify registered voters who are eligible to vote in an election.”.

(c) EFFECTIVE DATE.—Section 301(e) of such Act (52 U.S.C. 21081(e)), as redesignated by subsection (b), is amended by striking the period at the end and inserting the following: “, or, with respect to any requirements relating to electronic poll books, on and after January 1, 2020.”.

**SEC. 205. PRE-ELECTION REPORTS ON VOTING SYSTEM USAGE.**

(a) **REQUIRING STATES TO SUBMIT REPORTS.**—Title III of the Help America Vote Act of 2002 (52 U.S.C. 21081 et seq.) is amended by inserting after section 301 the following new section:

**“SEC. 301A. PRE-ELECTION REPORTS ON VOTING SYSTEM USAGE.**

“(a) **REQUIRING STATES TO SUBMIT REPORTS.**—Not later than 120 days before the date of each regularly scheduled general election for Federal office, the chief State election official of a State shall submit a report to the Commission containing a detailed voting system usage plan for each jurisdiction in the State which will administer the election, including a detailed plan for the usage of electronic poll books and other equipment and components of such system.

“(b) **EFFECTIVE DATE.**—Subsection (a) shall apply with respect to the regularly scheduled general election for Federal office held in November 2020 and each succeeding regularly scheduled general election for Federal office.”.

(b) **CONFORMING AMENDMENT RELATING TO ENFORCEMENT.**—Section 401 of such Act (52 U.S.C. 21111) is amended by striking “sections 301, 302, and 303” and inserting “subtitle A of title III”.

(c) **CLERICAL AMENDMENT.**—The table of contents of such Act is amended by inserting after the item relating to section 301 the following new item:

“Sec. 301A. Pre-election reports on voting system usage.”.

**SEC. 206. STREAMLINING COLLECTION OF ELECTION INFORMATION.**

Section 202 of the Help America Vote Act of 2002 (52 U.S.C. 20922) is amended—

(1) by striking “The Commission” and inserting “(a) **IN GENERAL.**—The Commission”; and

(2) by adding at the end the following new subsection:

“(b) **WAIVER OF CERTAIN REQUIREMENTS.**—Subchapter I of chapter 35 of title 44, United States Code, shall not apply to the collection of information for purposes of maintaining the clearinghouse described in paragraph (1) of subsection (a).”.

## **TITLE III—USE OF VOTING MACHINES MANUFACTURED IN THE UNITED STATES**

**SEC. 301. USE OF VOTING MACHINES MANUFACTURED IN THE UNITED STATES.**

Section 301(a) of the Help America Vote Act of 2002 (52 U.S.C. 21081(a)), as amended by section 104, section 105, and section 203, is further amended by adding at the end the following new paragraph:

“(10) **VOTING MACHINE REQUIREMENTS.**—By not later than the date of the regularly scheduled general election for Federal office occurring in November 2022, each State shall seek to ensure that any voting machine used in such election and in any subsequent election for Federal office is manufactured in the United States.”.

## **TITLE IV—SEVERABILITY**

**SEC. 401. SEVERABILITY.**

If any provision of this Act or amendment made by this Act, or the application of a provision or amendment to any person or circumstance, is held to be unconstitutional, the remainder of this Act and amendments made by this Act, and the application of the provisions and amendment to any person or circumstance, shall not be affected by the holding.

### PURPOSE AND SUMMARY

H.R. 2722, the “Securing America’s Federal Elections Act” or the “SAFE Act,” will improve the resilience of election infrastructure used in Federal elections.

The legitimacy of our representative system of self-government rests on every eligible voter casting a ballot with confidence that it will count as cast. Aging equipment, under-resourced jurisdictions, and interference by foreign entities or non-state actors leave the system vulnerable to exploitation that undermines confidence

in election outcomes. Ineffective and vulnerable equipment can also discourage participation in Federal elections.

H.R. 2722 provides critical resources to states and localities to bolster election infrastructure, including necessary funds to replace aging voting equipment with voter-verified paper ballot voting systems and implement additional cybersecurity protocols. The bill also helps states and localities plan for future elections by providing ongoing maintenance funding on a biannual basis. The legislation provides grant programs for states to implement required risk-limiting audits, a best practice audit system that confirms election outcomes with a high degree of confidence.

The legislation also institutes accountability for election technology vendors so that they abide by cybersecurity standards, including agreeing to report known or suspect security incidents involving election infrastructure.

The SAFE Act will also spur innovation by awarding grants for research and development that will improve the accessibility of election infrastructure. One such grant program will study and report on accessible paper ballot verification mechanisms for individuals with disabilities, voters with difficulties in literacy, and voters whose primary language is not English.

#### BACKGROUND AND NEED FOR LEGISLATION

##### *Significant Vulnerabilities in Nation's Election Infrastructure*

In 2016, Russian hackers targeted state voting systems, and sought to infiltrate voter registration databases and the networks of election technology vendors. This attack exposed the numerous vulnerabilities in our nation's election infrastructure. Many states have not kept pace with changing voting technology. Some of the most significant vulnerabilities are outlined below:

##### *Paperless Machines*

Although there is no evidence that vote counts were altered in the 2016 election, voting machines remain vulnerable to attack. In 2017, at DefCon, one of the world's largest, longest-running, and best-known hacker conferences, 25 pieces of election equipment were successfully breached by participants with little prior knowledge and limited tools.<sup>1</sup> These issues are exacerbated by the fact that in 2016, twenty percent of Americans cast their ballot on voting machines that do not have any kind of paper backup, according to the Brennan Center for Justice.<sup>2</sup> In other words, if these paperless machines were hacked, it would be nearly impossible to tell.<sup>3</sup>

<sup>1</sup>Matt Blaze et al., *DEFCON 25 Voting Machine Hacking Village: Rep. on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*, at pg. 4 (2017) <https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf>.

<sup>2</sup>Lawrence Norden and Ian Vandewalker, *Securing Elections From Foreign Interference*, at pg. 11 (June 29, 2017), <https://www.brennancenter.org/publication/securing-elections-foreign-interference>.

<sup>3</sup>Eric Geller, *Virginia Bars Voting Machines Considered Top Hacking Target*, POLITICO (Sept. 8, 2017) <http://www.politico.com/story/2017/09/08/virginia-election-machines-hacking-target-242492>.

### *Need to Replace Aging Voting Equipment*

In at least 40 states, elections are carried out using voting machines that were purchased more than a decade ago.<sup>4</sup> Aging voting equipment creates at least three problems. First, older systems are increasingly difficult to maintain and are more likely to fail.<sup>5</sup> Second, many use outdated hardware and software and some are no longer manufactured.<sup>6</sup> For example, some state officials have “had to turn to eBay to find critical components like dot-matrix printer ribbons, decades old storage devices and analog modems. Aging systems also frequently rely on unsupported software, like Windows XP and 2000, which may not receive regular security patches and are thus more vulnerable to the latest methods of cyberattack.”<sup>7</sup> Finally, many jurisdictions are using voting equipment that predates federal certification and testing programs, which render them particularly susceptible to major flaws and cybersecurity vulnerabilities.<sup>8</sup> These systems disproportionately lack voter-marked paper ballots.<sup>9</sup>

### *Need for Risk-Limiting Audits*

The best way to determine whether a machine has been hacked, or mis-programmed, is to conduct a post-election, risk-limiting audit. Currently, 34 states and the District of Columbia require post-election audits of paper records; however, experts note that some of those audits are insufficient to determine whether anyone tampered with the election results.<sup>10</sup> Instead, experts recommend that states implement risk-limiting audits. A risk-limiting audit is a process that involves hand counting a certain number of ballots, using advanced statistical methods, to determine with a high degree of certainty that the reported election outcome is accurate. The number of ballots that are counted by hand is determined by many factors, including the margin of victory in the election. If the initial count determines that the election results are accurate, the audit stops. If the initial count is insufficient to confirm the election result, a larger sample of ballots is hand counted. This process continues until the election results can be confirmed. If there is never enough evidence to confirm the election results, a full hand count would be conducted.<sup>11</sup>

### *Election Technology Vendors*

Another significant vulnerability comes from election technology vendors. Many states purchase their voting systems

<sup>4</sup>Brennan Center for Justice, *New Analysis Shows Voting Machines Remain Vulnerable Ahead of 2020 Elections*, (Mar. 5, 2019) <https://www.brennancenter.org/press-release/new-analysis-shows-voting-machines-remain-vulnerable-ahead-2020-election>

<sup>5</sup>Written Testimony of Lawrence D. Norden, Deputy Director, Brennan Center for Justice at NYU School of Law, Hearing: “Election Security,” May 8, 2019, pg. 4 (hereinafter “Norden Testimony”).

<sup>6</sup>*Id.* at 5.

<sup>7</sup>*Id.*

<sup>8</sup>*Id.*

<sup>9</sup>*Id.*

<sup>10</sup>*National Conference of State Legislators, Post-Election Audits, Jan. 3, 2019* available at <http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx>

<sup>11</sup>*Risk-Limiting Audits Working Group, Risk-Limiting Post-Election Audits: Why and How*, at pg. 5, (Jennie Bretschneider et al. eds., 1.1 version, 2012) <https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf>.

from third-party vendors are not subject to regulations requiring them to use cybersecurity best practices. In addition, election vendors are not currently required to inform any federal agency or state election official in the event of a cyberattack. The Congressional Task Force on Election Security found that “the election technology industry is dominated by three firms whose products cover approximately 92% of the total eligible voter population.”<sup>12</sup> Accordingly, this consolidation presents a security risk in that “there is no meaningful competitive pressure from the suppliers to the vendors,” and “no incentive for election technology vendors to prioritize security. This problem is compounded by the lack of regulation in this area.”<sup>13</sup>

*Cybersecurity Training:*

States and localities also face the daunting task of training hundreds, if not thousands, of election officials, IT staff, and poll workers on cybersecurity and risk mitigation. The success of spear-phishing campaigns in the 2016 election demonstrate the urgent need for better cybersecurity training. Finally, many state chief information officers do not assist with election systems, and states often cannot afford or cannot find IT workers to help with state and local election information technology infrastructure.

*Maintaining and Upgrading IT Infrastructure*

States need money to replace outdated technology, including voter registration databases. The Help America Vote Act (HAVA) requires states to create and maintain a statewide, computerized voter registration database.<sup>14</sup> According to the Brennan Center, in at least 41 states, these systems were created at least ten years ago.<sup>15</sup> In Illinois, for example, Russian hackers successfully breached the databases and attempted, but failed, to alter and delete voting records.<sup>16</sup> The most significant threat posed by vulnerable voter registration databases is that an attacker could alter, delete, or add voter registration records which would then cause profound chaos on Election Day and potentially change the results of the election. Had the attackers successfully changed voting records in Illinois, voters would have arrived at the polls on Election Day to discover that they were not registered. This could lead “scores of voters to cast provisional ballots, leading to long lines, undermining faith in the fairness of an election, and creating a major administrative headache to accurately count votes after the polls closed.”<sup>17</sup> Alternatively, an attacker could add fake voters to the rolls, allowing for fraudulent votes to be cast.

<sup>12</sup> Congressional Task Force on Election Security, Final Report (January 2018), pg. 31. <https://homeland.house.gov/sites/democrats.homeland.house.gov/files/documents/TFESReport.pdf>.

<sup>13</sup> *Id.* (citing Penn Warton Pub. Policy Initiative, *The Warton School, University of Pennsylvania, The Business of Voting*, pgs. 11–13, 20 (2017) <https://publicpolicy.wharton.upenn.edu/live/files/270-the-business-of-voting>).

<sup>14</sup> Help America Vote Act of 2002, 52 U.S.C. § 21083.

<sup>15</sup> Norden & Vandewalker, 19.

<sup>16</sup> Callum Borchers, *What We Know About the 21 States Targeted by Russian Hackers*, The Washington Post (Sept. 23, 2017) [https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm\\_term=.c296117b25d4](https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?utm_term=.c296117b25d4).

<sup>17</sup> Norden & Vandewalker, at pg. 16.

In light of the threats and vulnerabilities facing state election systems, then-Secretary of Homeland Security Jeh Johnson in January, 2017 designated election systems as “critical infrastructure” which gives state election officials priority access to Department of Homeland Security (“DHS”) services.

In response to the 2016 attacks, then-Leader Pelosi established the Congressional Task Force on Election Security led by Committee on House Administration then-Ranking Member Robert Brady and then-Ranking Member Bennie G. Thompson. The Task Force engaged with election stakeholders, including cybersecurity and election infrastructure experts, to ensure the health and security of election systems. In February 2018, the Task Force released its report recommending the replacement of paperless voting machines with paper ballot voting systems; risk-limiting audits; upgraded IT infrastructure (including voter registration databases) with ongoing maintenance; requirements that election technology vendors secure their voting systems; Intelligence Community pre-election threat assessments and coordination with federal and state officials; ongoing DHS designation of election infrastructure as critical infrastructure; and prioritized cybersecurity training at the state level.

In March 2019, the Brennan Center for Justice issued an analysis of the current state of voting technology in the United States.<sup>18</sup> Local election officials in 254 jurisdictions across 37 states confirmed to the report’s authors that they “plan to purchase new voting equipment in the near future. For some, the need to make these replacements was extremely urgent: 121 officials in 31 states told [the Brennan Center] they must replace their equipment before the 2020 election. Two-thirds of these officials reported that they do not have the adequate funds to do so, even after the distribution of additional HAVA funds from Congress.”<sup>19</sup> Moreover, “[a]lmost every election official who responded that they planned on replacing voting equipment soon stated that their hope was to find new machines that produce voter-verified paper backups that could be used in a recount or audit.”<sup>20</sup> Finally, per the Brennan Center survey, election officials said their priority would be hiring more IT support staff, particularly at the local level.<sup>21</sup>

#### *Post-2016 Developments*

The Mueller Report<sup>22</sup> largely confirmed what was already known about Russian interference in the 2016 election. It also revealed that at least one Florida county had been breached by hackers. In recent months, several Trump administration officials, and one former official, have made public comments emphasizing the seriousness of the threat and urgent need for action. They are unequivocal in their assessment that foreign interference will continue in the lead up to the 2020 election.

<sup>18</sup> Lawrence Norden and Andrea Córdova, *Voting Machines at Risk: Where We Stand Today* (March 5, 2019), <https://www.brennancenter.org/analysis/voting-machines-risk-where-we-stand-today>.

<sup>19</sup> *Id.*

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

<sup>22</sup> Report on the Investigation into Russian Interference in the 2016 Presidential Election, Special Counsel Robert S. Mueller, III, Washington, D.C., March, 2019.

*The Mueller Report*

The Mueller Report confirmed that Russian hackers targeted state election administrators and election vendors. An excerpt of the redacted Mueller Report that addresses state election infrastructure is reproduced below:

In addition to targeting individuals involved in the Clinton Campaign, GRU officers also targeted individuals and entities involved in the administration of the elections. Victims included U.S. state and local entities, such as state boards of elections (SBOEs), secretaries of state, and county governments, as well as individuals who worked for those entities. The GRU also targeted private technology firms responsible for manufacturing and administering election-related software and hardware, such as voter registration software and electronic polling stations. The GRU continued to target these victims through the elections in November 2016. While the investigation identified evidence that the GRU targeted these individuals and entities, the Office did not investigate further. The Office did not, for instance, obtain or examine servers or other relevant items belonging to these victims. The Office understands that the FBI, the U.S. Department of Homeland Security, and the states have separately investigated that activity.

By at least the summer of 2016, GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as “SQL injection,” by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents). In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE’s website. The GRU then gained access to a database containing information on millions of registered Illinois voters, and extracted data related to thousands of U.S. voters before the malicious activity was identified.

GRU officers [REDACTED] scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers [REDACTED] for vulnerabilities on websites of more than two dozen states. [REDACTED]. Similar [REDACTED] for vulnerabilities continued through the election.

Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of [REDACTED], a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible

for administering the 2016 U.S. election. The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer. The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.<sup>23</sup>

*Director of National Intelligence “Worldwide Threat Assessment of the U.S. Intelligence Community.”*

In January 2019, Dan Coats, the Director of National Intelligence, offered the Intelligence Community’s 2019 assessment of threats to national security.<sup>24</sup> The report states that:

Our adversaries and strategic competitors probably already are looking to the 2020 US elections as an opportunity to advance their interests . . . [They] also may seek to use cyber means to directly manipulate or disrupt election systems—such as by tampering with voter registration or disrupting the vote tallying process—either to alter data or to call into question our voting process. Russia in 2016 and unidentified actors as recently as 2018 have already conducted cyber activity that has targeted US election infrastructure, but we do not have any intelligence reporting to indicate any compromise of our nation’s election infrastructure that would have prevented voting, changed vote counts, or disrupted the ability to tally votes.

*Former Secretary of Homeland Security Kirstjen Nielsen*

In April 2019, *The New York Times* reported that President Trump’s chief of staff, Mick Mulvaney, told former Homeland Security Secretary Kirstjen Nielsen not to mention “in front of the president” anything about her preparations for “new and different Russian forms of interference in the 2020 election.”<sup>25</sup> In July 2018, she said in remarks to the National Association of Secretaries of State that there were “no indications that Russia is targeting the 2018 U.S. midterms at a scale or scope to match their activities in 2016,” but that she “consistently observe[d] malicious cyber activity from various actors against U.S. election infrastructure.”<sup>26</sup> She also said that “there is little doubt that adversaries and non-state actors continue to view elections as a target for cyber and influence operations.”<sup>27</sup> According to the *Times*, Nielsen “eventually gave up

<sup>23</sup> *Ibid.*, Volume One, pg. 50–51 (March 2019).

<sup>24</sup> Daniel R. Coats, *Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*, Jan. 29, 2019, pg. 7, <https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf>.

<sup>25</sup> Eric Schmitt et al., *In Push for 2020 Election Security, Top Official Was Warned: Don’t Tell Trump*, *New York Times* (April 24, 2019), <https://www.nytimes.com/2019/04/24/us/politics/russia-2020-election-trump.html>.

<sup>26</sup> Department of Homeland Security, “Secretary of Homeland Security Kirstjen Nielsen NASS Conference Remarks: As Prepared for Delivery,” <https://www.dhs.gov/news/2018/07/16/nass-conference-remarks-prepared-delivery> (release date July 16, 2018).

<sup>27</sup> *Id.*

on her effort to organize a White House meeting of cabinet secretaries to coordinate a strategy to protect next year's elections. As a result, the issue did not gain the urgency or widespread attention that a president can command. And it meant that many Americans remain unaware of the latest versions of Russian interference."<sup>28</sup>

*FBI Director Christopher Wray*

Also in April 2019, FBI Director Christopher Wray called Russia's interference efforts in American elections a "significant counterintelligence threat."<sup>29</sup> *The New York Times* reported that he said in remarks to the Council on Foreign Relations that "our adversaries are going to keep adapting and upping their game. . . . So we are very much viewing 2018 as just kind of a dress rehearsal for the big show in 2020. . . . What has pretty much continued unabated is the use of social media, fake news, propaganda, false personae, etc. to spin us up, pit us against each other, to sow divisiveness and discord, to undermine America's faith in democracy. That is not just an election-cycle threat. It is pretty much a 365-day-a-year-threat."<sup>30</sup>

*Attorney General William Barr's Testimony*

At a May 1, 2019 hearing of the Senate Judiciary Committee, Chairman Lindsey Graham asked Attorney General Barr if he would recommend that the Judiciary Committee "and every other committee of Congress do our best to harden our infrastructure against future Russian attacks?" Barr replied, "Absolutely, yes."<sup>31</sup>

*The Role of the Election Assistance Commission*

On April 4, 2019, Committee on House Administration Chairperson Lofgren sent a letter to the Election Assistance Commission (EAC) seeking information about the Commission, with a particular focus on the work the EAC was doing to help states secure their elections. In response to that letter, the EAC sent a letter to Chairperson Lofgren on May 1, 2019 and reported the following regarding its election security activities: "As the 2020 Presidential Election approaches, providing election security tools and resources to state and local officials remains one of the EAC's most important responsibilities."<sup>32</sup> In addition to distributing the \$380 million in HAVA grants dedicated to election security in FY2018, the EAC noted several other initiatives it has undertaken in relation to election security. Specifically, it notes its work testing and federally certifying voting systems, "providing hands-on security and post-election audit trainings, producing security-focused resources, disseminating security best-practices information and checklists to state and local election officials, as well as hosting widely attended forums that feature security experts as speakers."<sup>33</sup>

The EAC has conducted a variety of these exercises throughout the country. For example, the EAC provided 11 separate training

<sup>28</sup> Schmitt et al.

<sup>29</sup> Julian A. Barnes and Adam Goldman, *F.B.I. Warns of Russian Interference in 2020 Race and Boosts Counterintelligence Operations*, N.Y. Times (April 26, 2019), <https://www.nytimes.com/2019/04/26/us/politics/fbi-russian-election-interference.html>.

<sup>30</sup> *Id.*

<sup>31</sup> U.S. Senate Committee on the Judiciary, Hearing: "The Department of Justice's Investigation of Russian Interference with the 2016 Presidential Election," May 1, 2019.

<sup>32</sup> Letter from the Election Assistance Commission to Chairperson Zoe Lofgren, May 1, 2019.

<sup>33</sup> *Id.*

sessions on Election Technology and Security for 600 election officials in nine states, provided post-election audit assistance and training across five states, offered white papers and best-practices checklists on securing election infrastructure to all states, and hosted two summits attended by hundreds of attendees to hear first-hand from election security and intelligence experts. In sum, the EAC's role has been to convene local and state elections officials with those experts positioned to aid them with their unique concerns, while also serving as a clearinghouse for best practices, and providing proactive analysis of what information all states might need and benefit from, based on incoming inquiries from some states.

The EAC also noted that staff and Commissioners routinely take part in Critical Infrastructure activities; they also serve as members of the Government Coordinating Council, and work closely with the Sector Coordinating Council. They also consistently coordinate with DHS and other federal partners, such as the Department of Defense's Federal Voting Assistance Program, to create and distribute resources for voters about trusted sources for election information and other security related topics.

*H.R. 2722—The SAFE Act*

H.R. 2272 provides the necessary resources to states to begin the process of upgrading and maintaining safe, resilient election infrastructure. Many of its provisions reflect the recommendations of the Congressional Task Force on Election Security.

First, H.R. 2260 authorizes \$600 million in grants to assist states in securing election infrastructure and transitioning to required voter-verified paper-based systems. The grants will require jurisdictions to use individual, durable, voter-verified paper ballots that are counted by hand or read by an optical character recognition device or other counting device. The National Academy of Sciences, Engineering, and Medicine concluded last year that systems lacking voter-marked paper ballots “should be removed from service as soon as possible.”<sup>34</sup> The Committee on House Administration heard from various experts during an Election Security hearing that replacing paperless systems with paper-based systems is a critical policy priority.<sup>35</sup> The “bridge between the voter and correctly reported outcomes requires a physical artifact as evidence of the voter's intent, and a process for checking. That artifact is typically the paper ballot,” wrote Marian Schneider of Verified Voting.<sup>36</sup> Dr. Joseph Lorenzo Hall of the Center for Democracy and Technology wrote that while “states and local jurisdictions continue to make progress updating their outdated voting technologies with newer systems that keep an auditable voter verifiable paper record, it is important to prioritize the continuing replacement of paperless direct-recording electronic (DRE) systems. DRE systems are not ‘software-independent’ systems, are unauditible, and as such unsuit-

<sup>34</sup> Norden Testimony at pg. 5.

<sup>35</sup> Written Testimony of Jocelyn Benson, Michigan Secretary of State, Hearing: “Election Security,” May 8, 2019 (hereinafter “Benson Testimony”); Written Testimony of Dr. Joseph Lorenzo Hall, Chief Technologist, The Center for Democracy & Technology, Hearing: “Election Security,” May 8, 2019 (hereinafter “Hall Testimony”); Norden Testimony; Written Testimony of Marian K. Schneider, President, Verified Voting, Hearing: “Election Security,” May 8, 2019 (hereinafter “Schneider Testimony”).

<sup>36</sup> Schneider Testimony at pg. 4.

able for government elections.”<sup>37</sup> Moreover, until there is adequate funding, some jurisdictions that use paperless systems will continue to do so because “1) some jurisdictions have already purchased paperless systems in the recent past and have no available resources to purchase new systems, and/or 2) these kinds of systems are unfortunately still available for sale.”<sup>38</sup>

The funding can also be used to carry out cyber and risk mitigation training; security risk and vulnerability assessments of a state’s election infrastructure; maintenance of election infrastructure, including addressing identified risks and vulnerabilities; increased technical support for information technology infrastructure; enhanced cybersecurity and operations of information technology systems; and enhancements to the cybersecurity of voter registration systems, among other things.

The SAFE Act also provides states with an ongoing stream of funding (\$175 million biannually for fiscal years 2020, 2022, 2024, and 2026) to assist with maintenance of election infrastructure. This will provide a predictable, stable, and reliable source of funds to better secure our elections. Michigan Secretary of State Jocelyn Benson testified before the Committee on House Administration that “[m]ost states purchased new voting machines and established statewide voter registration databases using funding made available through HAVA in the years following the law’s enactment. As those resources ran out, however, election technology began to age at the same time as technology was advancing at a rapid pace.”<sup>39</sup>

H.R. 2722 also requires states to administer risk-limiting audits, which the EAC shall pay to States the amount of the costs. States “vary widely in the effectiveness of post-election audits processes.”<sup>40</sup> Post-election audits are an important corollary to using voter-verified paper ballots—namely, because “[p]aper records will not prevent programming errors, software bugs, or the insertion of corrupt software into voting systems. Voter-marked paper ballots will only have real security value if they are used to check and confirm electronic tallies.”<sup>41</sup> The most robust type of audit are risk-limiting audits.<sup>42</sup> According to Jerome Lovato of the Election Assistance Commission, “a risk-limiting audit (RLA) provides strong statistical evidence that the election outcome is right and has a high probability of correcting a wrong outcome.”<sup>43</sup> One witness at the Committee on House Administration’s election security hearing compared the importance of risk-limiting audits to the “public policy invention” of the secret ballot at the turn of the 20th century.<sup>44</sup>

H.R. 2722 fosters accountability for election technology vendors. This is important because “there is almost no federal oversight of private vendors that design and maintain the systems that allow us to determine who can vote, how they vote, what voters see when they cast their vote, how votes are counted and how those vote totals are communicated to the public. In fact, there are more federal regulations for ballpoint pens and magic markers than there are

<sup>37</sup> Hall Testimony at pg. 4.

<sup>38</sup> *Id.* at 5.

<sup>39</sup> Benson Testimony, pg. 6.

<sup>40</sup> Schneider Testimony, pg. 8.

<sup>41</sup> Norden Testimony, pg. 7.

<sup>42</sup> Schneider Testimony, pg. 4.

<sup>43</sup> Jerome Lovato, *Defining and Piloting Risk-Limiting Audits*, Election Assistance Commission (Aug. 9, 2018), <https://www.eac.gov/defining-and-piloting-risk-limiting-audits/>.

<sup>44</sup> Hall Testimony, pg. 5.

for voting systems and other parts of our election infrastructure.”<sup>45</sup> H.R. 2722 address this by limiting state expenditures on goods and services with grant monies to purchases from “qualified election infrastructure vendors.” H.R. 2722 tasks the EAC, in coordination with DHS, to establish criteria for “qualified election infrastructure vendor” status, which must include maintaining IT infrastructure in a manner that is consistent with the best practices provided by the EAC’s Technical Guidelines Development Committee. Moreover, vendors must be owned and controlled by a citizen or permanent resident of the United States and disclose any sourcing outside the United States for parts of the election infrastructure. It must also agree to independent security testing by the EAC and DHS. Finally, H.R. 2722 requires vendors to report any known or suspected security incidents involving election infrastructure.

The ongoing threat of interference in Federal elections continues to demand robust guardrails to reinforce other cybersecurity best practices. The legislation establishes cybersecurity requirements that will apply equally to current and future technology to protect the necessity that every vote is counted as cast. For example, H.R. 2722 prohibits the use of wireless communications devices and internet connectivity in certain voting systems or devices involving ballot marking, tabulation, or aggregation, or upon which ballots are marked by voters.

H.R. 2722 also includes open source provisions, requiring use of software and hardware for which information is disclosed by manufacturers. This will allow cybersecurity experts—and the public—to thoroughly vet the security of elections systems, regardless of the technology used.

The legislation provides funds to study and report on accessible paper ballot verification mechanisms, including for individuals with disabilities, voters with difficulties in literacy, and voters whose primary language is not English.

Ultimately, H.R. 2722 is an important investment in the integrity of self-government. It reflects an ongoing commitment to the security of the machinery of democracy—the infrastructure and systems to ensure, with necessary confidence, that votes are counted as cast at each Federal election.

#### HEARINGS

For the purposes of section 103(i) of H. Res. 6 of the 116th Congress the following hearings were used to develop or consider H.R. 2722:

(1) On Wednesday, May 8, 2019 the Committee held a hearing titled “Election Security.” The following witnesses testified: Mr. Larry Norden, Brennan Center for Justice; Ms. Marian Schneider, Verified Voting; Mr. Joseph Lorenzo Hall, Center for Democracy and Technology; The Honorable Jocelyn Benson, Secretary of State, State of Michigan; and The Honorable John Merrill, Secretary of State, State of Alabama.

(2) On Tuesday, May 21, 2019, the Committee held a hearing titled “Oversight of the Election Assistance Commission.” The following witnesses testified: The Honorable Christy McCormick, Commissioner and Chairwoman, Election Assistance Commission,

<sup>45</sup>Norden Testimony, pg. 12.

accompanied by The Honorable Benjamin Hovland, Commissioner and Vice Chair, Election Assistance Commission; The Honorable Don Palmer, Commissioner, Election Assistance Commission; and The Honorable Thomas Hicks, Commissioner, Election Assistance Commission.

(3) On Thursday, February 14, 2019, the Committee held a hearing titled “For the People: Our American Democracy.” The following witnesses testified: Mr. Chiraag Bains, Director of Legal Strategies, Demos; Ms. Wendy Weiser, Director, Democracy Program, Brennan Center for Justice at NYU School of Law; Mr. Fred Wertheimer, President, Democracy 21; The Honorable Kim Wyman, Secretary of State, State of Washington; Mr. Alejandro Rangel-Lopez, Senior at Dodge City High School, Dodge City Kansas, and plaintiff in *LULAC & Rangel-Lopez v. Cox*; Mr. Peter Earle, Wisconsin Civil Rights Trial Lawyer; Mr. Brandon A. Jessup, Data Science and Information Systems Professional; Executive Director, Michigan Forward; and David Keating, President, Institute for Free Speech.

#### COMMITTEE CONSIDERATION

On Friday, June 21, 2019, the Committee met in open session and ordered the bill, H.R. 2722, as amended, favorably reported to the House by voice vote, a quorum being present.

#### COMMITTEE VOTES

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following rollcall votes occurred during the Committee’s consideration of H.R. 2722:

1. The Lofgren amendment in the nature of a substitute to H.R. 2722 (H.R. 2722 as amended) agreed to by a rollcall vote of 6 to 3. The vote was as follows:

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Ms. Lofgren .....	X	.....	.....	Mr. Davis (IL) .....	.....	X	.....
Mr. Raskin .....	X	.....	.....	Mr. Walker .....	.....	X	.....
Ms. Davis (CA) .....	X	.....	.....	Mr. Loudermilk .....	.....	X	.....
Mr. Butterfield .....	X	.....	.....				
Ms. Fudge .....	X	.....	.....				
Mr. Aguilar .....	X	.....	.....				

2. A substitute amendment offered by Mr. Davis of Illinois (Amendment 01) was defeated to by a rollcall vote of 5 to 3. The vote was as follows:

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Ms. Lofgren .....	.....	X	.....	Mr. Davis (IL) .....	X	.....	.....
Mr. Raskin .....	.....	.....	.....	Mr. Walker .....	X	.....	.....
Ms. Davis (CA) .....	.....	X	.....	Mr. Loudermilk .....	X	.....	.....
Mr. Butterfield .....	.....	X	.....				
Ms. Fudge .....	.....	X	.....				
Mr. Aguilar .....	.....	X	.....				

3. An amendment offered by Mr. Davis of Illinois (Amendment 02) to strike subtitle A of title I was defeated by a rollcall vote of 3 to 6. The vote was as follows:

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Ms. Lofgren .....		X	.....	Mr. Davis (IL) .....	X	.....	.....
Mr. Raskin .....		X	.....	Mr. Walker .....	X	.....	.....
Ms. Davis (CA) .....		X	.....	Mr. Loudermilk .....	X	.....	.....
Mr. Butterfield .....		X	.....				
Ms. Fudge .....		X	.....				
Mr. Aguilar .....		X	.....				

4. An amendment offered by Mr. Loudermilk (Amendment 03) to strike section 105 was defeated to by a rollcall vote of 6 to 2. The vote was as follows:

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Ms. Lofgren .....		X	.....	Mr. Davis (IL) .....	X	.....	.....
Mr. Raskin .....		X	.....	Mr. Walker .....		.....	.....
Ms. Davis (CA) .....		X	.....	Mr. Loudermilk .....	X	.....	.....
Mr. Butterfield .....		X	.....				
Ms. Fudge .....		X	.....				
Mr. Aguilar .....		X	.....				

5. An amendment offered by Mr. Loudermilk (Amendment 04) to strike subtitle B of title I and insert new subtitle B with was defeated to by a rollcall vote of 6 to 2. The vote was as follows:

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Ms. Lofgren .....		X	.....	Mr. Davis (IL) .....	X	.....	.....
Mr. Raskin .....		X	.....	Mr. Walker .....		.....	.....
Ms. Davis (CA) .....		X	.....	Mr. Loudermilk .....	X	.....	.....
Mr. Butterfield .....		X	.....				
Ms. Fudge .....		X	.....				
Mr. Aguilar .....		X	.....				

6. An amendment offered by Mr. Davis of Illinois (Amendment 05) to require a State match of 25 percent of any grant received by a State for obtaining compliant paper ballot voting systems and carrying out voting system security improvements was defeated to by a rollcall vote of 6 to 3. The vote was as follows:

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Ms. Lofgren .....		X	.....	Mr. Davis (IL) .....	X	.....	.....
Mr. Raskin .....		X	.....	Mr. Walker .....	X	.....	.....
Ms. Davis (CA) .....		X	.....	Mr. Loudermilk .....	X	.....	.....
Mr. Butterfield .....		X	.....				
Ms. Fudge .....		X	.....				
Mr. Aguilar .....		X	.....				

7. An amendment offered by Mr. Walker (Amendment 06) to add new title IV “Prohibiting Ballot Harvesting” was defeated to by a rollcall vote of 6 to 3. The vote was as follows:

Representative	Yea	Nay	Present	Representative	Yea	Nay	Present
Ms. Lofgren .....		X	.....	Mr. Davis (IL) .....	X	.....	.....
Mr. Raskin .....		X	.....	Mr. Walker .....	X	.....	.....
Ms. Davis (CA) .....		X	.....	Mr. Loudermilk .....	X	.....	.....
Mr. Butterfield .....		X	.....				
Ms. Fudge .....		X	.....				
Mr. Aguilar .....		X	.....				

## COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII and clause (2)(b)(1) of rule X of the Rules of the House of Representatives, the Committee's oversight findings and recommendations are reflected in the descriptive portions of this report

## STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

The objective of H.R. 2722, as amended, is to protect elections for public office by providing financial support and enhanced security for the infrastructure used to carry out such elections.

## NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

## EARMARKS AND TAX AND TARIFF BENEFITS

H.R. 2722 contains no congressional earmarks, limited tax benefits, or limited tariff benefits as described in clauses 9(e), 9(f), and 9(g) of House rule XXI.

## COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate on H.R. 2722, as amended, prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

## CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate for H.R. 2722, as amended, provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

U.S. CONGRESS,  
CONGRESSIONAL BUDGET OFFICE,  
*Washington, DC, June 25, 2019.*

Hon. ZOE LOFGREN,  
*Chairperson, Committee on House Administration,  
House of Representatives, Washington, DC.*

DEAR MADAM CHAIRPERSON: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 2722, the SAFE Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Matthew Pickford.

Sincerely,

MARK P. HADLEY  
(For Phillip L. Swagel, Director).

Enclosure.

<b>At a Glance</b>			
<b>H.R. 2722, SAFE Act</b>			
As ordered reported by the House Committee on House Administration on June 21, 2019			
By Fiscal Year, Millions of Dollars	2019	2019-2024	2019-2029
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Deficit Effect	0	0	0
Spending Subject to Appropriation (Outlays)	0	1,125	n.e.
Statutory pay-as-you-go procedures apply?	No	<b>Mandate Effects</b>	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2030?	No	Contains intergovernmental mandate?	<b>Yes, Under Threshold</b>
		Contains private-sector mandate?	<b>No</b>
n.e. = not estimated.			

The bill would

- Authorize appropriations for grants to improve voting systems
- Amend federal statutes regarding the security of elections
- Impose an intergovernmental mandate by requiring states to submit a report on the usage plan for voting systems in each jurisdiction in the state

Estimated budgetary effects would primarily stem from

- Authorizing appropriations for grants to states to enhance the security of voting systems

*Bill Summary*

H.R. 2722 would authorize the appropriation of more than \$1.1 billion over the 2019–2024 period, primarily for states and localities to improve voting technology. The bill also would set standards for election technology vendors.

*Estimated Federal Cost*

The estimated budgetary effect of H.R. 2722 is shown in Table 1. The costs of the legislation fall within budget function 800 (general government).

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 2722

	By fiscal year, millions of dollars—						
	2019	2020	2021	2022	2023	2024	2019–2024
<b>Voting System Grants:</b>							
Estimated Authorization <sup>a</sup> .....	0	775	0	175	0	175	1,125
Estimated Outlays .....	0	580	195	130	45	130	1,080
<b>Other Provisions:</b>							
Estimated Authorization .....	0	5	20	0	20	0	45
Estimated Outlays .....	0	5	20	0	20	0	45
<b>Total Changes:</b>							
Estimated Authorization <sup>a</sup> .....	0	780	20	175	20	175	1,170

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 2722—Continued

	By fiscal year, millions of dollars—						
	2019	2020	2021	2022	2023	2024	2019–2024
Estimated Outlays .....	0	585	215	130	65	130	1,125

<sup>a</sup>H.R. 2722 would authorize the appropriation of \$600 million in fiscal year 2019. Because most appropriations acts for 2019 have already been completed, for this cost estimate CBO has shown that authorized amount in 2020 along with \$175 million specifically authorized for 2020.

### *Basis of Estimate*

For this estimate, CBO assumes that the bill will be enacted near the end of 2019 and that the specified and estimated amounts will be appropriated for each fiscal year beginning in 2020. H.R. 2722 would authorize the appropriation of \$600 million in fiscal year 2019 for voting system grants. CBO expects that H.R. 2722 will not be enacted until after the appropriations acts for fiscal year 2019 are completed. Therefore, CBO has assumed that the \$600 million authorized to be appropriated in 2019 would apply to fiscal year 2020. Estimated outlays are based on historical patterns for existing and similar activities.

Assuming appropriation of the specified and estimated amounts, CBO estimates that implementing the bill would cost about \$1.1 billion over the 2019–2024 period.

**Voting System Grants.** Section 111 would authorize the appropriation of \$600 million in 2019 and \$175 million in each of fiscal years 2020, 2022, 2024, and 2026 for grants for state and localities to improve voting systems. CBO estimates that those grants would cost \$1.1 billion over the 2020–2024 period, and about \$200 million after 2024.

**Other Provisions.** H.R. 2722 also would authorize appropriations for several other activities aimed at improving the security of elections. The bill would authorize grants for states to audit elections by using statistical evidence to determine whether election outcomes are accurate. Additionally, the bill would require the National Science Foundation to study paper ballots and the best practices associated with such ballots and would require the Election Assistance Commission to study the use of paper or digital ballots. H.R. 2722 would also authorize the appropriation of \$5 million to prepare the required studies and whatever amounts are necessary for the auditing grants to states. CBO estimates that implementing those provisions would cost \$45 million over the 2020–2024 period.

Pay-As-You-Go considerations: None.

Increase in long-term deficits: None.

### *Mandates*

Section 4 of the Unfunded Mandates Reform Act (UMRA) excludes from the application of that act any legislative provision that enforces constitutional rights of individuals. CBO has determined that title III as well as certain provisions of titles I and II fall within such exclusion because they would enforce constitutionally-protected voting rights.

Section 205 would impose an intergovernmental mandate by requiring states to submit a report on the usage plan for voting systems in each jurisdiction in the state, which would include details

on how each jurisdiction would use electronic poll books and other equipment. Because states report extensively on their election activities and have previously reported similar information, CBO estimates the cost of the mandate would be small and fall below the threshold established in UMRA (\$82 million in 2019, adjusted annually for inflation).

H.R. 2722 contain no private-sector mandates as defined in UMRA.

Estimate prepared by: Federal Costs: Matthew Pickford; Mandates: Rachel Austin.

Estimate reviewed by: Kim Cawley, Chief, Natural and Physical Resources; Susan Willie, Chief, Mandates Unit; H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis; Theresa Gullo, Assistant Director for Budget Analysis.

#### FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates regarding H.R. 2722, as amended, prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

#### NON-DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of House rule XIII, the committee states that no provision of this resolution establishes or reauthorizes a program of the Federal Government known to be duplicative of another Federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

#### ADVISORY COMMITTEE STATEMENT

H.R. 2722 does not establish or authorize any new advisory committees.

#### APPLICABILITY TO LEGISLATIVE BRANCH

H.R. 2722 does not apply to terms and conditions of employment or to access to public services or accommodations within the legislative branch.

#### SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

##### *Section 1. Short title; table of contents*

Subsection (a) of this section would provide the short title of H.R. 2722, as amended, as the “Securing America’s Federal Elections Act” or the “SAFE Act.” Subsection (b) would provide the table of contents

TITLE I—FINANCIAL SUPPORT FOR ELECTION  
INFRASTRUCTURE

Subtitle A—Voting System Security Improvement Grants

Part 1—Promoting Accuracy, Integrity, and Security Through  
Voter-Verified Permanent Paper Ballot

*Section 101. Short title*

Would provide the short title for Subsection A as the “Voter Confidence and Increased Accessibility Act of 2019.”

*Section 102. Paper ballot and manual counting requirements*

This section would require individual, durable, voter-verified, paper ballots. Votes must be counted by hand or read by an optical character recognition device or other counting device. In addition, this section would define “individual, durable, voter-verified, paper ballot” as a paper ballot marked by the voter by hand or marked through the use of a nontabulating ballot marking device or system, so long as the option exists to mark by hand. The voting system must provide voters an opportunity to correct his or her ballot before the ballot is preserved. Ballots would not be preserved in any manner that makes it possible to associate a voter to the ballot without the voter’s consent. Further, a paper ballot constitutes the official ballot and shall be used for any recount or audit, and shall be counted by hand in the event of a recount or audit for any federal election.

This section would require that paper ballots cast be considered the true and correct record of votes cast in the event of any inconsistency or irregularities between hand-counted ballots and any electronic vote tallies. Applies paper ballot requirement to all ballots cast in elections for federal office, including ballots cast by absent uniformed services voters and overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act.

Finally, this section provides a special rule for treatment of disputes when paper ballots have been shown, by clear and convincing evidence, to be compromised, and where compromised ballots exist in such numbers that the results of the election could be changed by them. Provides that the appropriate remedy shall be made in accordance with applicable state law, except that the electronic tally may not be used as the exclusive basis for determining the official certified result.

*Section 103. Accessibility and ballot verification for individuals with disabilities*

This section would require the use of at least one voting system at each polling place that is equipped for individuals with disabilities (including nonvisual and enhanced visual accessibility for the blind and visually impaired, and enhanced manual accessibility for the mobility and dexterity impaired). Further, it would require that, for federal elections occurring six years or more after the enactment of the SAFE Act, each polling place to have at least one voting system for voters with disabilities that marks ballots identical in size, ink, and paper stock to ballots used by voters without accessibility needs, that also marks the ballot in a manner such

that it is not readily discernable whether the ballot was marked by machine or hand, and that combines ballots produced from the accessible voter system with other ballots in a manner that prevents identification of which ballots were cast by which system. It would require that such system be available for use by any voter who requests its use, and, for federal elections occurring six years or more after the enactment of the SAFE Act, must allow the voter to privately and independently verify the accuracy of the paper ballot by presenting, in an accessible form, the vote selections in the same manner they would appear for any vote tabulation or auditing. Clarifies that nothing in this section shall be construed to prohibit the use of an accessible ballot that may be printed or marked by the voter at home.

Finally, this section would authorize to be appropriated \$5,000,000 for the Director of the National Science Foundation to make grants to at least three entities to study, test, and develop accessible paper ballot voting, verification, and casting mechanisms, and best practices to enhance accessibility of paper ballot voting and verification for voters with disabilities, voters whose primary language is not English, and voters who have difficulties with literacy. It would establish grant eligibility requirements and provides that any technology developed under these grants shall be treated as non-proprietary and made available to the public. It would direct the Director to coordinate these activities with grants for technology improvements. It would require that when adopting any voluntary guidance regarding accessibility of the paper ballot verification requirements for individuals with disabilities, the Election Assistance Commission (EAC) shall apply the same accessibility standards applicable under this subtitle. Finally, it would permit use of funds for protection and advocacy systems to support actions to enforce election-related disability access.

#### *Section 104. Durability and readability requirements for ballots*

This section would require that all voter-verified ballots are printed on durable paper that is able to maintain the accuracy and integrity of the ballot over repeated handling, including retaining and preserving information printed on the ballot for a period of 22 months. It would require that all voter-verified paper ballots completed through the use of a ballot marking device to be clearly readable by the voter without assistance (other than eyeglasses or other personal vision enhancing devices) and by an optical character recognition device or other device equipped for individuals with disabilities.

#### *Section 105. Paper ballot printing requirements*

This section would require that all paper ballots used in an election for federal office shall be printed in the United States on recycled paper manufactured in the United States.

#### *Section 106. Study and report on optimal ballot design*

This section would require the EAC to conduct a study of the best ways to design election ballots, including paper ballots and electronic or digital ballots, to minimize confusion and user errors, and to provide a report to Congress on the results of such study not later than January 1, 2020.

*Section 107. Effective date for new requirements*

This section would add an effective date to the Help America Vote Act of 2002 (HAVA) relating to requirement first imposed on a state or jurisdiction by the provisions of this subtitle. It would also allow jurisdictions using certain systems such as certain paper record printers (including voter-verified paper record printers attached to direct recording electronic voting machines) to delay implementation to 2022 regarding select requirements, so long as certain contingencies are in place during the delay, including the option of having voters cast a vote using a blank pre-printed paper ballot which the voter may mark by hand and which is not produced by the direct recording electronic voting machine or other such system, and requiring that such paper ballot be counted as a regular and not provisional ballot. It would further require each polling place display notice of paper ballot option, and training of poll workers about said option, all in effect so long as delayed compliance is in effect.

## Part 2—Grants to Carry Out Improvements

*Section 111. Grants for obtaining compliant paper ballot voting systems and carrying out voting system security improvements*

This section would amend subtitle D of title II of HAVA by adding the following new sections under Part 7—Grants for obtaining compliant paper ballot voting systems and carrying out voting system security improvements, adding the following new sections:

## Section 297. Grants for Obtaining Compliant Paper Ballot Voting Systems and Carrying Out Voting System Security Improvements

This new section would direct the EAC to make available grants for eligible states to (1) replace voting systems that are not compliant paper ballot voting systems under the Voter Confidence and Increased Accessibility Act of 2019, or those which are compliant but do not meet the most recent voluntary voting system guidelines promulgated by the EAC prior to the November 2020 federal elections, as well as (2) carry out voting system security improvements, and (3) implement and model best practices for ballot design, ballot instructions, and ballot testing.

In addition, it would establish that grants made to states under this section shall be of an amount the EAC determines to be appropriate, except that a state shall not receive less than the product of \$1 and the average of the number of individuals who cast votes in any of the two most recent regularly scheduled general elections for federal office held in the state. In the event that Congress appropriates insufficient funds to provide States the amount directed per the above, the EAC shall make a pro rata reduction to ensure that the entire appropriated amount is distributed to the states. It would provide factors for the EAC to consider in awarding excess funds to a state in the event of a surplus of appropriated funds. It would also provide that, to the greatest extent practicable, an eligible state which receives a grant to replace a voting system under

this section shall ensure such replacement system is capable of administering a system of ranked choice voting.

Section 297A. Voting System Security Improvements Described

This new section would define voting system security improvements as: (1) The acquisition of goods and services from qualified election infrastructure vendors by purchase, lease, or such other arrangements as may be appropriate; (2) cyber and risk mitigation training; (3) a security risk and vulnerability assessment of the state's election infrastructure which is carried out by a provider of cybersecurity services under a contract entered into between the chief state election official and the provider; (4) the maintenance of election infrastructure, including addressing risks and vulnerabilities which are identified under either of the security risk and vulnerability assessments described in paragraph (3), except that none of the funds provided under this part may be used to renovate or replace a building or facility which is used primarily for purposes other than the administration of elections for public office; (5) providing increased technical support for any information technology infrastructure that the chief state election official deems to be part of the state's election infrastructure or designates as critical to the operation of the state's election infrastructure; (6) enhancing the cybersecurity and operations of the information technology infrastructure described in paragraph (4); and (7) enhancing the cybersecurity of voter registration systems.

Further, it would define a "qualified election infrastructure vendor" as any person who provides, supports, or maintains, or who seeks to provide, support, or maintain, election infrastructure on behalf of a state, unit of local government, or election agency who meets certain criteria established by the Chair of the EAC and the Secretary of Homeland Security.

Additionally, this new section would direct the Chair of the EAC and the Secretary of Homeland Security to include the following in the criteria a person must meet to be considered a "qualified election infrastructure vendor": (A) the vendor must be owned and controlled by a citizen or permanent resident of the United States; (B) the vendor must disclose to the Chair and the Secretary, and to the chief state election official of any state to which the vendor provides any goods and services with funds provided under this part, of any sourcing outside the United States for parts of the election infrastructure; (C) the vendor agrees to ensure that the election infrastructure will be developed and maintained in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee; (D) the vendor agrees to maintain its information technology infrastructure in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee; (E) the vendor agrees to meet the notification requirement defined herein with respect to any known or suspected cybersecurity incidents involving any of the goods and services provided by the vendor pursuant to a grant under this part; and (F) the vendor agrees to permit independent security test-

ing by the EAC and by the Secretary of the goods and services provided by the vendor pursuant to a grant under this part.

It would also establish cybersecurity incident reporting requirements that a vendor meets if, upon learning of a potential cybersecurity incident involving any of the goods and services provided by the vendor, the vendor promptly assesses whether such incident occurred and notifies the Chair of the EAC and the Secretary of Homeland Security as soon as practicable but not later than three days after becoming aware of the potential incident. The vendor must also inform any potentially impacted election agency within three days and cooperate with the agency in providing any further notifications necessary. The vendor must provide ongoing updates to the Chair of the EAC, the Secretary of Homeland Security, and the impacted election agency.

Finally, this new section would provide that the notification the vendor must provide to the Chair of the EAC, the Secretary of Homeland Security, and the affected election agency must include the following: (1) the date, time, and time zone when the election cybersecurity incident began, if known; (2) the date, time, and time zone when the election cybersecurity incident was detected; (3) the date, time, and duration of the election cybersecurity incident; (4) the circumstances of the election cybersecurity incident, including the specific election infrastructure systems believed to have been accessed and information acquired, if any; (5) any planned and implemented technical measures to respond to and recover from the incident; (6) in the case of any notification which is an update to a prior notification, any additional material information relating to the incident, including technical data, as it becomes available.

#### Section 297B. Eligibility of States

This new section would provide that to be eligible for a grant, in its application to the EAC, a state must: (1) describe how it will use the grant to carry out the activities authorized under this part; (2) certify and assure that, not later than 5 years after receiving the grant, the state will carry out voting system security improvements as described above; and (3) provide other information and assurances as the EAC may require.

#### Section 297C. Reports to Congress

This new section would require the EAC to, not later than 90 days after the end of each fiscal year, submit a report to the appropriate congressional committees, including the Committees on Homeland Security, House Administration, and the Judiciary of the House of Representatives and the Committees on Homeland Security and Governmental Affairs, the Judiciary, and Rules and Administration of the Senate, on the activities carried out with the funds provided under this part.

#### Section 297D. Authorization of Appropriations

This new section would provide an authorization of appropriations of \$600,000,000 for FY 2019 and further authorize

\$175 million for each of the fiscal years 2020, 2022, 2024, and 2026. It would also provide that any amounts appropriated shall remain available until expended.

*Section 112. Coordination of voting system security activities with use of requirements payments and election administration requirements under Help America Vote Act of 2002*

This section would amend HAVA to add the Secretary of Homeland Security or the Secretary's designee to the Board of Advisors of the EAC. It would also add a representative from the Department of Homeland Security to the Technical Guidelines Development Committee.

It would direct the EAC to consult with the Department of Homeland Security in conducting periodic studies on election administration and adds to the objectives of the periodic studies ensuring the integrity of elections against interference through cyber means.

This section would amend the allowable uses of requirements payments under HAVA to include voting system security improvements, including cyber training for election officials, technical support, enhancing cybersecurity of information systems, and enhancing cybersecurity of voter registration databases. Requires states to include protection of election infrastructure into their state plans for use of payments developed pursuant to 52 U.S.C. 21004.

Additionally, it would require that the Committee responsible for composing the state plans developed pursuant to 52 U.S.C. 21004 be composed of a representative group from the state's counties, cities, towns, Indian tribes, and to represent rural as well as urban areas.

Finally, it would require states to undertake measures to prevent and deter cybersecurity incidents, as identified by the EAC, the Secretary of Homeland Security, and the Technical Guidelines Development Committee, of computerized voter registration databases.

*Section 113. Incorporation of definitions*

This section would amend HAVA to include the definitions of "cybersecurity incident" (6 U.S.C. 148), "election infrastructure," "election agency," and "State" (States, D.C., Puerto Rico, Guam, American Samoa, U.S. Virgin Islands, Northern Mariana Islands).

Subtitle B—Risk-Limiting Audits

*Section 121. Risk-limiting audits*

This section would amend title III of HAVA by adding the following new section:

Section 303A. Risk-limiting audits

This new section would define, among other terms, "risk-limiting audit" to mean a post-election process that has at least a 95% probability of correcting the reported outcome of an election if the reported outcome is incorrect; will not change the outcome if the reported outcome is the correct outcome; and involves a manual adjudication of voter intent (meaning a direct inspection and determination, by humans, of ballot choices

marked by voters) from some or all validly-cast ballots in an election.

It would require that, not later than one year after the enactment of this section, each state's chief election official must establish several specific rules and procedures for conducting risk-limiting audits. Establishes effective date by requiring that requirements of this section, including risk-limiting audits, be complied with for the first regularly scheduled federal election held more than one year following the enactment of the SAFE Act and for each subsequent election.

It would require that if a risk-limiting audit corrects the reported outcome of an election contest, the state will use the results of the manual adjudication of voter intent conducted within the risk-limiting audit as the official results of the election.

Additionally, it would exempt from risk-limiting audit requirement those election contests where a state or jurisdiction conducts a full recount through a manual adjudication of voter intent.

Finally, it would require states to publish public report after completion of risk-limiting audit and at least five days before the relevant election contest is certified, demonstrating results of the audit and information necessary to confirm that audit was properly conducted. Notes all data must be published in machine-readable, open data formats, and that data published must not compromise the anonymity of votes.

*Section 122. Funding for conducting post-election risk-limiting audits*

This section would amend subtitle D of title II of HAVA by adding the following:

Part 8—Funding for Post-Election Risk-Limiting Audits.

Section 298. Payments for post-election risk-limiting audits.

This new section would establish that the EAC will pay to states the amount of eligible post-election audit costs, where such costs are those paid or incurred by the state or local government for the conduct of any risk-limiting audit for a federal election occurring after the date of enactment of this section, and any equipment, software, or services needed to conduct such audit.

It would require the EAC to establish rules and procedures for states to submit eligible costs, and establishes a formula to adjust payments to states if the amounts appropriated are insufficient to pay for all eligible post-election costs submitted by states. Authorizes the appropriation of such sums as are necessary to carry out this part, and establishes that appropriated amounts remain available until expended.

*Section 123. GAO analysis of effects of audits*

This section would provide that no later than 6 months after the first federal elections held for which states must conduct risk-limiting audits, requires that the Comptroller General of the United States conduct an analysis of the extent to which risk-limiting au-

dits have improved election administration and the security of election infrastructure in states that received grants. It would direct the Comptroller General to submit a report to relevant congressional committees regarding such analysis.

TITLE II—Promoting Cybersecurity Through Improvements in  
Election Administration

*Section 201. Voting system cybersecurity requirements*

This section would establish ballot tabulating methods where voting systems must tabulate ballots by hand or use optical scanning devices that meet enumerated criteria (except in limited circumstances).

It would require that optical scanning devices must (1) be designed and built in such a manner that it is impossible for the device to add or change a voter's selection on a printed or marked ballot; (2) be capable of exporting its data in a machine-readable, open data standard format; (3) consist of hardware components certified by section 2216 of the Homeland Security Act that also conform to a hardware component manifest that includes point-of-origin and upstream hardware supply chain information that has been provided to the EAC, Department of Homeland Security, and each state where the device is used, and further may be shared with independent experts for cybersecurity analysis; (4) utilize technology that prevents device operation if any hardware requirements are not met; (5) only operate using software for which the source code, compilation parameters, and build tools have been provided to the EAC, Department of Homeland Security, and the chief state election official of each state where the device is used, and such software may be shared with independent experts for cybersecurity analysis; (5) utilize technology that prevents the software running should requirements of (5) be unmet; (7) utilizes technology that allows stakeholders to verify that the software running on the device meets certain requirements; and (8) contains such other security requirements as the Director of Cybersecurity and Infrastructure Security require.

It would allow the Director to waive some requirements for a period not to exceed two years, and requires internet publication of information related to any such waiver. Establishes effective date of these requirements for federal elections in 2024 and federal elections thereafter.

This section would prohibit the use of wireless communications devices in systems or devices. Specifically, it would prohibit systems or devices on which ballots are programmed or designed, or ballots are marked (except as necessary for voting by individuals with disabilities), or upon which votes are cast, tabulated, or aggregated, from containing, using, or being accessible by wireless, power-line, or concealed communication device, effective in the federal elections of 2020.

Additionally, it would prohibit connection of voting system to the internet by requiring that no system or device upon which ballot marking devices or optical scanners are configured, or ballots are marked by voters, or votes cast, tabulated, or aggregated, shall be connected to the internet or any other communications network at any time, effective in the federal elections of 2020.

Finally, it would establish additional cybersecurity standards for certain ballot marking devices. It would prohibit states from using ballot marking devices unless an independent laboratory in a simulated election scenario finds there is less than a five percent chance that an ordinary voter using the device would not report any difference between her vote selection and the vote selection printed on the ballot by the ballot marking device. It would lay out the requirements for valid simulated election scenario and establishes effective date in the federal elections of November 2022 and each subsequent federal election. It would establish procedures and requirements for testing and certification of ballot marking devices, per an application submitted to the EAC. It would allow for the EAC to submit findings to an independent board for review and prohibits the EAC from charging fees associated with testing and certification to state or jurisdiction, or developer or manufacturer of ballot marking device, or any other relevant party.

*Section 202. Testing of existing voting systems to ensure compliance with election cybersecurity guidelines and other guidelines*

This section would amend HAVA to require the EAC to provide, not later than nine months before regularly scheduled federal elections, for the testing by accredited laboratories under this section of the voting system hardware and software certified for use in the most recent such election, on the basis of the most recent voting system guidelines applicable to such hardware or software (including election cybersecurity guidelines) issued under this Act. It would require the EAC to decertify any hardware or software the EAC determines does not meet the most recent guidelines. This section applies to the regularly scheduled general election for federal office held in November 2020 and each succeeding regularly scheduled general election for federal office.

Additionally, it would amend HAVA to require the Technical Guidelines Development Committee within the EAC, within six months of enactment of the SAFE Act, to issue election cybersecurity guidelines, including standards and best practices for procuring, maintaining, testing, operating, and updating election systems to prevent and deter cybersecurity incidents.

*Section 203. Requiring use of software and hardware for which information is disclosed by manufacturer*

This section would amend HAVA to establish that, in operating voting systems relevant to federal elections, states may only use software for which the source code is disclosed by the manufacturer and made publicly available online for use, excepting that the manufacturer may prohibit usage of the software primarily intended for commercial advantage or private compensation, unrelated to carrying out legitimate research or cybersecurity activity. Further, it would except widely-used operating system software and cybersecurity software not specific to voting systems.

It would prohibit use of voting systems in federal elections unless the manufacturer discloses online the hardware used to operate the system. It would add additional restrictions and disclosure requirements for custom-made or altered hardware, including that the design of such hardware must be made publicly available online for use, except that a manufacturer may prohibit use for commercial

advantage or private compensation, unrelated to carrying out legitimate research or cybersecurity activity. It would make this requirement effective for federal elections held in 2020 or any succeeding year.

*Section 204. Treatment of electronic poll books as part of voting systems*

This section would amend HAVA to include electronic poll books as part of voting systems. It would define electronic poll books as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used: (1) to retain the list of registered voters at a polling location, or vote center, or other location at which voters cast votes in an election for federal office; and (2) to identify registered voters who are eligible to vote in an election. It would make this requirement effective January 1, 2020.

*Section 205. Pre-election reports on voting system usage*

This section would require the chief state election official of each state to submit a report to the EAC containing a detailed voting system usage plan for each jurisdiction which will administer an election, including a plan for usage of electronic poll books and other system components, no later than 120 days prior to any regularly scheduled election for federal office, and would make this effective for November 2020 federal elections and subsequent elections.

*Section 206. Streamlining collection of election information*

This section would waive certain federal information policy requirements of subchapter I of chapter 35 of title 44, United States Code for purposes of maintaining the clearinghouse described in this section.

TITLE III—Use of Voting Machines Manufactured in the United States

*Section 301. Use of voting machines manufactured in the United States*

This section would amend HAVA by establishing that, not later than the regularly scheduled general election for federal office of 2022, each state shall seek to ensure that any voting machine used in that election and any election thereafter is manufactured in the United States.

TITLE IV—Severability

*Section 401. Severability*

This section would establish severability such that the application of the provisions of this Act and amendments made by this Act shall not be affected by a holding finding any provision of the Act or amendment made by the Act unconstitutional.

## CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, and existing law in which no change is proposed is shown in roman):

**HELP AMERICA VOTE ACT OF 2002****SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

(a) **SHORT TITLE.**—This Act may be cited as the “Help America Vote Act of 2002”.

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

Sec. 1. Short title; table of contents.

\* \* \* \* \*

**TITLE II—COMMISSION**

\* \* \* \* \*

**Subtitle B—Testing, Certification, Decertification, and Recertification of Voting System Hardware and Software; *Ballot Marking Devices***

Sec. 231. Certification and testing of voting systems.

Sec. 232. *Testing and certification of ballot marking devices.*

**Subtitle C—Studies and Other Activities To Promote Effective Administration of Federal Elections**

\* \* \* \* \*

Sec. 247. *Study and report on accessible paper ballot verification mechanisms.*

**[Sec. 247.]** Sec. 248. Consultation with Standards Board and Board of Advisors.

**Subtitle D—Election Assistance**

\* \* \* \* \*

**PART 7—GRANTS FOR OBTAINING COMPLIANT PAPER BALLOT VOTING SYSTEMS AND CARRYING OUT VOTING SYSTEM SECURITY IMPROVEMENTS**

Sec. 297. *Grants for obtaining compliant paper ballot voting systems and carrying out voting system security improvements.*

Sec. 297A. *Voting system security improvements described.*

Sec. 297B. *Eligibility of States.*

Sec. 297C. *Reports to Congress.*

Sec. 297D. *Authorization of appropriations.*

**PART 8—FUNDING FOR POST-ELECTION RISK-LIMITING AUDITS**

Sec. 298. *Payments for post-election risk-limiting audits.*

**TITLE III—UNIFORM AND NONDISCRIMINATORY ELECTION TECHNOLOGY AND ADMINISTRATION REQUIREMENTS****Subtitle A—Requirements**

Sec. 301. Voting systems standards.

Sec. 301A. *Pre-election reports on voting system usage.*

Sec. 302. Provisional voting and voting information requirements.

Sec. 303. Computerized statewide voter registration list requirements and requirements for voters who register by mail.

Sec. 303A. *Risk-limiting audits.*

**Subtitle B—Coverage of Commission Under Certain Laws and Programs**

\* \* \* \* \*

TITLE IX—MISCELLANEOUS PROVISIONS

【Sec. 901. State defined.】  
Sec. 901. Definitions.

\* \* \* \* \*

**TITLE II—COMMISSION**

**Subtitle A—Establishment and General Organization**

**PART 1—ELECTION ASSISTANCE COMMISSION**

\* \* \* \* \*

**SEC. 202. DUTIES.**

【The Commission】 (a) *IN GENERAL.*—*The Commission shall serve as a national clearinghouse and resource for the compilation of information and review of procedures with respect to the administration of Federal elections 【by】 and the security of election infrastructure by—*

(1) carrying out the duties described in part 3 (relating to the adoption of voluntary voting system guidelines), including the maintenance of a clearinghouse of information on the experiences of State and local governments in implementing the guidelines and in operating voting systems in general;

(2) carrying out the duties described in subtitle B (relating to the testing, certification, decertification, and recertification of voting system hardware and software *and ballot marking devices*);

(3) carrying out the duties described in subtitle C (relating to conducting studies and carrying out other activities to promote the effective administration of Federal elections);

(4) carrying out the duties described in subtitle D (relating to election assistance), and providing information and training on the management of the payments and grants provided under such subtitle;

(5) carrying out the duties described in subtitle B of title III (relating to the adoption of voluntary guidance); and

(6) developing and carrying out the Help America Vote College Program under title V.

(b) *WAIVER OF CERTAIN REQUIREMENTS.*—*Subchapter I of chapter 35 of title 44, United States Code, shall not apply to the collection of information for purposes of maintaining the clearinghouse described in paragraph (1) of subsection (a).*

\* \* \* \* \*

**PART 2—ELECTION ASSISTANCE COMMISSION STANDARDS BOARD AND BOARD OF ADVISORS**

\* \* \* \* \*

**SEC. 214. MEMBERSHIP OF BOARD OF ADVISORS.**

(a) *IN GENERAL.*—*The Board of Advisors shall be composed of 【37 members】 38 members appointed as follows:*

(1) Two members appointed by the National Governors Association.

(2) Two members appointed by the National Conference of State Legislatures.

(3) Two members appointed by the National Association of Secretaries of State.

(4) Two members appointed by the National Association of State Election Directors.

(5) Two members appointed by the National Association of Counties.

(6) Two members appointed by the National Association of County Recorders, Election Administrators, and Clerks.

(7) Two members appointed by the United States Conference of Mayors.

(8) Two members appointed by the Election Center.

(9) Two members appointed by the International Association of County Recorders, Election Officials, and Treasurers.

(10) Two members appointed by the United States Commission on Civil Rights.

(11) Two members appointed by the Architectural and Transportation Barrier Compliance Board under section 502 of the Rehabilitation Act of 1973 (29 U.S.C. 792).

(12) The chief of the Office of Public Integrity of the Department of Justice, or the chief's designee.

(13) The chief of the Voting Section of the Civil Rights Division of the Department of Justice or the chief's designee.

(14) The director of the Federal Voting Assistance Program of the Department of Defense.

(15) Four members representing professionals in the field of science and technology, of whom—

(A) one each shall be appointed by the Speaker and the Minority Leader of the House of Representatives; and

(B) one each shall be appointed by the Majority Leader and the Minority Leader of the Senate.

(16) Eight members representing voter interests, of whom—

(A) four members shall be appointed by the Committee on House Administration of the House of Representatives, of whom two shall be appointed by the chair and two shall be appointed by the ranking minority member; and

(B) four members shall be appointed by the Committee on Rules and Administration of the Senate, of whom two shall be appointed by the chair and two shall be appointed by the ranking minority member.

(17) *The Secretary of Homeland Security or the Secretary's designee.*

(b) MANNER OF APPOINTMENTS.—Appointments shall be made to the Board of Advisors under subsection (a) in a manner which ensures that the Board of Advisors will be bipartisan in nature and will reflect the various geographic regions of the United States.

(c) TERM OF SERVICE; VACANCY.—Members of the Board of Advisors shall serve for a term of 2 years, and may be reappointed. Any vacancy in the Board of Advisors shall be filled in the manner in which the original appointment was made.

(d) CHAIR.—The Board of Advisors shall elect a Chair from among its members.

\* \* \* \* \*

### PART 3—TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE

#### SEC. 221. TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE.

(a) ESTABLISHMENT.—There is hereby established the Technical Guidelines Development Committee (hereafter in this part referred to as the “Development Committee”).

(b) DUTIES.—

(1) IN GENERAL.—The Development Committee shall assist the Executive Director of the Commission in the development of the voluntary voting system guidelines.

(2) DEADLINE FOR INITIAL SET OF RECOMMENDATIONS.—The Development Committee shall provide its first set of recommendations under this section to the Executive Director of the Commission not later than 9 months after all of its members have been appointed.

(3) *ELECTION CYBERSECURITY GUIDELINES.*—*Not later than 6 months after the date of the enactment of the Securing America’s Federal Elections Act, the Development Committee shall issue election cybersecurity guidelines, including standards and best practices for procuring, maintaining, testing, operating, and updating election systems to prevent and deter cybersecurity incidents.*

(c) MEMBERSHIP.—

(1) IN GENERAL.—The Development Committee shall be composed of the Director of the National Institute of Standards and Technology (who shall serve as its chair), together with a group of 14 other individuals appointed jointly by the Commission and the Director of the National Institute of Standards and Technology, consisting of the following:

(A) An equal number of each of the following:

(i) Members of the Standards Board.

(ii) Members of the Board of Advisors.

(iii) Members of the Architectural and Transportation Barrier Compliance Board under section 502 of the Rehabilitation Act of 1973 (29 U.S.C. 792).

(B) A representative of the American National Standards Institute.

(C) A representative of the Institute of Electrical and Electronics Engineers.

(D) Two representatives of the National Association of State Election Directors selected by such Association who are not members of the Standards Board or Board of Advisors, and who are not of the same political party.

(E) *A representative of the Department of Homeland Security.*

**[(E)]** (F) Other individuals with technical and scientific expertise relating to voting systems and voting equipment.

(2) QUORUM.—A majority of the members of the Development Committee shall constitute a quorum, except that the De-

velopment Committee may not conduct any business prior to the appointment of all of its members.

(d) NO COMPENSATION FOR SERVICE.—Members of the Development Committee shall not receive any compensation for their service, but shall be paid travel expenses, including per diem in lieu of subsistence, at rates authorized for employees of agencies under subchapter I of chapter 57 of title 5, United States Code, while away from their homes or regular places of business in the performance of services for the Development Committee.

(e) TECHNICAL SUPPORT FROM NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.—

(1) IN GENERAL.—At the request of the Development Committee, the Director of the National Institute of Standards and Technology shall provide the Development Committee with technical support necessary for the Development Committee to carry out its duties under this subtitle.

(2) TECHNICAL SUPPORT.—The technical support provided under paragraph (1) shall include intramural research and development in areas to support the development of the voluntary voting system guidelines under this part, including—

(A) the security of computers, computer networks, and computer data storage used in voting systems, including the computerized list required under section 303(a);

(B) methods to detect and prevent fraud;

(C) the protection of voter privacy;

(D) the role of human factors in the design and application of voting systems, including assistive technologies for individuals with disabilities (including blindness) and varying levels of literacy; and

(E) remote access voting, including voting through the Internet.

(3) NO PRIVATE SECTOR INTELLECTUAL PROPERTY RIGHTS IN GUIDELINES.—No private sector individual or entity shall obtain any intellectual property rights to any guideline or the contents of any guideline (or any modification to any guideline) adopted by the Commission under this Act.

(f) PUBLICATION OF RECOMMENDATIONS IN FEDERAL REGISTER.—At the time the Commission adopts any voluntary voting system guideline pursuant to section 222, the Development Committee shall cause to have published in the Federal Register the recommendations it provided under this section to the Executive Director of the Commission concerning the guideline adopted.

\* \* \* \* \*

## **Subtitle B—Testing, Certification, Decertification, and Recertification of Voting System Hardware and Software; *Ballot Marking Devices***

### **SEC. 231. CERTIFICATION AND TESTING OF VOTING SYSTEMS.**

(a) CERTIFICATION AND TESTING.—

(1) **IN GENERAL.**—The Commission shall provide for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories.

(2) **OPTIONAL USE BY STATES.**—At the option of a State, the State may provide for the testing, certification, decertification, or recertification of its voting system hardware and software by the laboratories accredited by the Commission under this section.

(3) **TESTING TO ENSURE COMPLIANCE WITH GUIDELINES.**—

(A) **TESTING.**—*Not later than 9 months before the date of each regularly scheduled general election for Federal office, the Commission shall provide for the testing by accredited laboratories under this section of the voting system hardware and software which was certified for use in the most recent such election, on the basis of the most recent voting system guidelines applicable to such hardware or software (including election cybersecurity guidelines) issued under this Act.*

(B) **DECERTIFICATION OF HARDWARE OR SOFTWARE FAILING TO MEET GUIDELINES.**—*If, on the basis of the testing described in subparagraph (A), the Commission determines that any voting system hardware or software does not meet the most recent guidelines applicable to such hardware or software issued under this Act, the Commission shall decertify such hardware or software.*

(b) **LABORATORY ACCREDITATION.**—

(1) **RECOMMENDATIONS BY NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.**—Not later than 6 months after the Commission first adopts voluntary voting system guidelines under part 3 of subtitle A, the Director of the National Institute of Standards and Technology shall conduct an evaluation of independent, non-Federal laboratories and shall submit to the Commission a list of those laboratories the Director proposes to be accredited to carry out the testing, certification, decertification, and recertification provided for under this section.

(2) **APPROVAL BY COMMISSION.**—

(A) **IN GENERAL.**—The Commission shall vote on the accreditation of any laboratory under this section, taking into consideration the list submitted under paragraph (1), and no laboratory may be accredited for purposes of this section unless its accreditation is approved by a vote of the Commission.

(B) **ACCREDITATION LABORATORIES NOT ON DIRECTOR LIST.**—The Commission shall publish an explanation for the accreditation of any laboratory not included on the list submitted by the Director of the National Institute of Standards and Technology under paragraph (1).

(c) **CONTINUING REVIEW BY NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY.**—

(1) **IN GENERAL.**—In cooperation with the Commission and in consultation with the Standards Board and the Board of Advisors, the Director of the National Institute of Standards and Technology shall monitor and review, on an ongoing basis, the performance of the laboratories accredited by the Commission under this section, and shall make such recommendations to

the Commission as it considers appropriate with respect to the continuing accreditation of such laboratories, including recommendations to revoke the accreditation of any such laboratory.

(2) APPROVAL BY COMMISSION REQUIRED FOR REVOCATION.—The accreditation of a laboratory for purposes of this section may not be revoked unless the revocation is approved by a vote of the Commission.

(d) TRANSITION.—Until such time as the Commission provides for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories under this section, the accreditation of laboratories and the procedure for the testing, certification, decertification, and recertification of voting system hardware and software used as of the date of the enactment of this Act shall remain in effect.

**SEC. 232. TESTING AND CERTIFICATION OF BALLOT MARKING DEVICES.**

(a) *IN GENERAL.*—Any State or jurisdiction which intends to use a ballot marking device (other than a ballot marking device used exclusively to comply with the requirements of section 301(a)(3)) in an election for Federal office may submit an application to the Commission for testing and certification under this section.

(b) *APPLICATION, ASSIGNMENT, AND TESTING.*—

(1) *IN GENERAL.*—An application under subsection (a) shall be submitted not later than 18 months before the date of the election for Federal office in which the ballot marking device is intended to be used and shall contain such information as the Commission requires.

(2) *ASSIGNMENT.*—Upon receipt of an application for testing under this section, the Commission shall contract with a qualified independent user experience research laboratory for the testing of whether the ballot marking device intended to be used by the State or jurisdiction meets the requirements of section 301(a)(10)(B).

(3) *REQUIREMENTS FOR TESTING.*—Any contract described in paragraph (2) shall require the qualified independent user experience research laboratory to—

(A) not later than 30 days before testing begins, submit to the Commission for approval the protocol for the simulated election scenario used for testing the ballot marking device;

(B) use only protocols approved by the Commission in conducting such testing; and

(C) submit to the Commission a report on the results of the testing.

(4) *QUALIFIED INDEPENDENT USER EXPERIENCE RESEARCH LABORATORY.*—For purposes of this section:

(A) *IN GENERAL.*—The term “qualified independent user experience research laboratory” means a laboratory accredited under this subsection by the Election Assistance Commission in accordance with standards determined by the Commission, in consultation with the Director of the National Institute of Standards and Technology and the Secretary of Homeland Security.

(B) *CRITERIA.*—A laboratory shall not be accredited under this subsection unless such laboratory demonstrates that—

(i) no employee of, or individual with an ownership in, such laboratory has, or has had during the 5 preceding years, any financial relationship with a manufacturer of voting systems; and

(ii) any group of individuals conducting tests under this section collectively meet the following qualifications:

(I) *Experience designing and running user research studies and experiments using both qualitative and quantitative methodologies.*

(II) *Experience with voting systems.*

(c) *REVIEW BY INDEPENDENT BOARD.*—

(1) *IN GENERAL.*—The Commission shall submit for approval to an independent review board established under paragraph (3) the following:

(A) Any protocol submitted to the Commission under subsection (b)(3)(A).

(B) Any report submitted to the Commission under subsection (b)(3)(C).

(2) *FINAL APPROVAL.*—Not later than the date that is 12 months before the date of the election for Federal office in which a State or jurisdiction intends to use the ballot marking device, the independent review board shall report to the Commission on whether it has approved a report submitted under paragraph (1)(B).

(3) *INDEPENDENT REVIEW BOARD.*—

(A) *IN GENERAL.*—An independent review board established under this paragraph shall be composed of 5 independent scientists appointed by the Commission, in consultation with the Director of the National Institute of Standards and Technology.

(B) *QUALIFICATIONS.*—The members of the independent review board—

(i) shall have expertise and relevant peer-reviewed publications in the following fields: cognitive psychology, experimental design, statistics, and user experience research and testing; and

(ii) may not have, or have had during the 5 preceding years, any financial relationship with a manufacturer of voting systems.

(4) *PUBLICATION.*—The Commission shall make public—

(A) any protocol approved under this subsection;

(B) any report submitted under subsection (b)(3)(C); and

(C) any determination made by an independent review board under paragraph (2).

(d) *CERTIFICATION.*—If—

(1) a ballot marking device is determined by the qualified independent user experience research laboratory to meet the requirements of section 301(a)(7); and

(2) the report submitted under subsection (b)(3)(C) is approved by a majority of the members of the independent review board under subsection (d)(2),

then the Commission shall certify the ballot marking device.

(e) *PROHIBITION ON FEES.*—The Commission may not charge any fee to a State or jurisdiction, a developer or manufacturer of a ballot marking device, or any other person in connection with testing and certification under this section.

## **Subtitle C—Studies and Other Activities To Promote Effective Administration of Federal Elections**

### **SEC. 241. PERIODIC STUDIES OF ELECTION ADMINISTRATION ISSUES.**

(a) *IN GENERAL.*—On such periodic basis as the Commission may determine, **[the Commission shall]** *the Commission, in consultation with the Secretary of Homeland Security (as appropriate), shall* conduct and make available to the public studies regarding the election administration issues described in subsection (b), with the goal of promoting methods of voting and administering elections which—

(1) will be the most convenient, accessible, and easy to use for voters, including members of the uniformed services and overseas voters, individuals with disabilities, including the blind and visually impaired, and voters with limited proficiency in the English language;

(2) will yield the most accurate, secure, and expeditious system for voting and tabulating election results;

(3) will be nondiscriminatory and afford each registered and eligible voter an equal opportunity to vote and to have that vote counted; **[and]**

(4) *will be secure against attempts to undermine the integrity of election systems by cyber or other means; and*

**[(4)]** (5) will be efficient and cost-effective for use.

(b) *ELECTION ADMINISTRATION ISSUES DESCRIBED.*—For purposes of subsection (a), the election administration issues described in this subsection are as follows:

(1) Methods and mechanisms of election technology and voting systems used in voting and counting votes in elections for Federal office, including the over-vote and under-vote notification capabilities of such technology and systems.

(2) Ballot designs for elections for Federal office.

(3) Methods of voter registration, maintaining secure and accurate lists of registered voters (including the establishment of a centralized, interactive, statewide voter registration list linked to relevant agencies and all polling sites), and ensuring that registered voters appear on the voter registration list at the appropriate polling site.

(4) Methods of conducting provisional voting.

(5) Methods of ensuring the accessibility of voting, registration, polling places, and voting equipment to all voters, including individuals with disabilities (including the blind and visually impaired), Native American or Alaska Native citizens, and voters with limited proficiency in the English language.

(6) Nationwide statistics and methods of identifying, deterring, and investigating voting fraud in elections for Federal office.

(7) Identifying, deterring, and investigating methods of voter intimidation.

(8) Methods of recruiting, training, and improving the performance of poll workers.

(9) Methods of educating voters about the process of registering to vote and voting, the operation of voting mechanisms, the location of polling places, and all other aspects of participating in elections.

(10) The feasibility and advisability of conducting elections for Federal office on different days, at different places, and during different hours, including the advisability of establishing a uniform poll closing time and establishing—

(A) a legal public holiday under section 6103 of title 5, United States Code, as the date on which general elections for Federal office are held;

(B) the Tuesday next after the 1st Monday in November, in every even numbered year, as a legal public holiday under such section;

(C) a date other than the Tuesday next after the 1st Monday in November, in every even numbered year as the date on which general elections for Federal office are held; and

(D) any date described in subparagraph (C) as a legal public holiday under such section.

(11) Federal and State laws governing the eligibility of persons to vote.

(12) Ways that the Federal Government can best assist State and local authorities to improve the administration of elections for Federal office and what levels of funding would be necessary to provide such assistance.

(13)(A) The laws and procedures used by each State that govern—

(i) recounts of ballots cast in elections for Federal office;

(ii) contests of determinations regarding whether votes are counted in such elections; and

(iii) standards that define what will constitute a vote on each type of voting equipment used in the State to conduct elections for Federal office.

(B) The best practices (as identified by the Commission) that are used by States with respect to the recounts and contests described in clause (i).

(C) Whether or not there is a need for more consistency among State recount and contest procedures used with respect to elections for Federal office.

(14) The technical feasibility of providing voting materials in eight or more languages for voters who speak those languages and who have limited English proficiency.

(15) Matters particularly relevant to voting and administering elections in rural and urban areas.

(16) Methods of voter registration for members of the uniformed services and overseas voters, and methods of ensuring that such voters receive timely ballots that will be properly and expeditiously handled and counted.

(17) The best methods for establishing voting system performance benchmarks, expressed as a percentage of residual vote in the Federal contest at the top of the ballot.

(18) Broadcasting practices that may result in the broadcast of false information concerning the location or time of operation of a polling place.

(19) Such other matters as the Commission determines are appropriate.

(c) **REPORTS.**—The Commission shall submit to the President and to the Committee on House Administration of the House of Representatives and the Committee on Rules and Administration of the Senate a report on each study conducted under subsection (a) together with such recommendations for administrative and legislative action as the Commission determines is appropriate.

\* \* \* \* \*

**SEC. 247. STUDY AND REPORT ON ACCESSIBLE PAPER BALLOT VERIFICATION MECHANISMS.**

(a) **STUDY AND REPORT.**—*The Director of the National Science Foundation shall make grants to not fewer than 3 eligible entities to study, test, and develop accessible paper ballot voting, verification, and casting mechanisms and devices and best practices to enhance the accessibility of paper ballot voting and verification mechanisms for individuals with disabilities, for voters whose primary language is not English, and for voters with difficulties in literacy, including best practices for the mechanisms themselves and the processes through which the mechanisms are used.*

(b) **ELIGIBILITY.**—*An entity is eligible to receive a grant under this part if it submits to the Director (at such time and in such form as the Director may require) an application containing—*

(1) *certifications that the entity shall specifically investigate enhanced methods or devices, including non-electronic devices, that will assist such individuals and voters in marking voter-verified paper ballots and presenting or transmitting the information printed or marked on such ballots back to such individuals and voters, and casting such ballots;*

(2) *a certification that the entity shall complete the activities carried out with the grant not later than December 31, 2020; and*

(3) *such other information and certifications as the Director may require.*

(c) **AVAILABILITY OF TECHNOLOGY.**—*Any technology developed with the grants made under this section shall be treated as non-proprietary and shall be made available to the public, including to manufacturers of voting systems.*

(d) **COORDINATION WITH GRANTS FOR TECHNOLOGY IMPROVEMENTS.**—*The Director shall carry out this section so that the activities carried out with the grants made under subsection (a) are coordinated with the research conducted under the grant program carried out by the Commission under section 271, to the extent that the Director and Commission determine necessary to provide for the advancement of accessible voting technology.*

(e) **AUTHORIZATION OF APPROPRIATIONS.**—*There is authorized to be appropriated to carry out subsection (a) \$5,000,000, to remain available until expended.*

**SEC. [247.] 248. CONSULTATION WITH STANDARDS BOARD AND BOARD OF ADVISORS.**

The Commission shall carry out its duties under this subtitle in consultation with the Standards Board and the Board of Advisors.

**Subtitle D—Election Assistance**

**PART 1—REQUIREMENTS PAYMENTS**

**SEC. 251. REQUIREMENTS PAYMENTS.**

(a) **IN GENERAL.**—The Commission shall make a requirements payment each year in an amount determined under section 252 to each State which meets the conditions described in section 253 for the year.

(b) **USE OF FUNDS.**—

(1) **IN GENERAL.**—Except as provided in paragraphs (2) and (3), a State receiving a requirements payment shall use the payment only to meet the requirements of title III.

(2) **OTHER ACTIVITIES.**—A State may use a requirements payment to carry out other activities to improve the administration of elections for Federal office if the State certifies to the Commission that—

(A) the State has implemented the requirements of title III; or

(B) the amount expended with respect to such other activities does not exceed an amount equal to the minimum payment amount applicable to the State under section 252(c).

(3) **ACTIVITIES UNDER UNIFORMED AND OVERSEAS CITIZENS ABSENTEE VOTING ACT.**—A State shall use a requirements payment made using funds appropriated pursuant to the authorization under section 257(a)(4) only to meet the requirements under the Uniformed and Overseas Citizens Absentee Voting Act imposed as a result of the provisions of and amendments made by the Military and Overseas Voter Empowerment Act.

(4) **PERMITTING USE OF PAYMENTS FOR VOTING SYSTEM SECURITY IMPROVEMENTS.**—A State may use a requirements payment to carry out any of the following activities:

(A) *Cyber and risk mitigation training.*

(B) *Providing increased technical support for any information technology infrastructure that the chief State election official deems to be part of the State's election infrastructure or designates as critical to the operation of the State's election infrastructure.*

(C) *Enhancing the cybersecurity and operations of the information technology infrastructure described in subparagraph (B).*

(D) *Enhancing the security of voter registration databases.*

(c) **RETROACTIVE PAYMENTS.**—

(1) **IN GENERAL.**—Notwithstanding any other provision of this subtitle, including the maintenance of effort requirements of section 254(a)(7), a State may use a requirements payment as a reimbursement for costs incurred in obtaining voting equipment which meets the requirements of section 301 if the

State obtains the equipment after the regularly scheduled general election for Federal office held in November 2000.

(2) SPECIAL RULE REGARDING MULTIYEAR CONTRACTS.—A State may use a requirements payment for any costs for voting equipment which meets the requirements of section 301 that, pursuant to a multiyear contract, were incurred on or after January 1, 2001, except that the amount that the State is otherwise required to contribute under the maintenance of effort requirements of section 254(a)(7) shall be increased by the amount of the payment made with respect to such multiyear contract.

(d) ADOPTION OF COMMISSION GUIDELINES AND GUIDANCE NOT REQUIRED TO RECEIVE PAYMENT.—Nothing in this part may be construed to require a State to implement any of the voluntary voting system guidelines or any of the voluntary guidance adopted by the Commission with respect to any matter as a condition for receiving a requirements payment.

(e) SCHEDULE OF PAYMENTS.—As soon as practicable after the initial appointment of all members of the Commission (but in no event later than 6 months thereafter), and not less frequently than once each calendar year thereafter, the Commission shall make requirements payments to States under this part.

(f) LIMITATION.—A State may not use any portion of a requirements payment—

- (1) to pay costs associated with any litigation, except to the extent that such costs otherwise constitute permitted uses of a requirements payment under this part; or
- (2) for the payment of any judgment.

\* \* \* \* \*

**SEC. 254. STATE PLAN.**

(a) IN GENERAL.—The State plan shall contain a description of each of the following:

(1) How the State will use the requirements payment to meet the requirements of title III, and, if applicable under section 251(a)(2), to carry out other activities to improve the administration of elections[.], *including the protection of election infrastructure.*

(2) How the State will distribute and monitor the distribution of the requirements payment to units of local government or other entities in the State for carrying out the activities described in paragraph (1), including a description of—

(A) the criteria to be used to determine the eligibility of such units or entities for receiving the payment; and

(B) the methods to be used by the State to monitor the performance of the units or entities to whom the payment is distributed, consistent with the performance goals and measures adopted under paragraph (8).

(3) How the State will provide for programs for voter education, election official education and training, and poll worker training which will assist the State in meeting the requirements of title III.

(4) How the State will adopt voting system guidelines and processes which are consistent with the requirements of section 301.

(5) How the State will establish a fund described in subsection (b) for purposes of administering the State's activities under this part, including information on fund management.

(6) The State's proposed budget for activities under this part, based on the State's best estimates of the costs of such activities and the amount of funds to be made available, including specific information on—

(A) the costs of the activities required to be carried out to meet the requirements of title III;

(B) the portion of the requirements payment which will be used to carry out activities to meet such requirements; and

(C) the portion of the requirements payment which will be used to carry out other activities.

(7) How the State, in using the requirements payment, will maintain the expenditures of the State for activities funded by the payment at a level that is not less than the level of such expenditures maintained by the State for the fiscal year ending prior to November 2000.

(8) How the State will adopt performance goals and measures that will be used by the State to determine its success and the success of units of local government in the State in carrying out the plan, including timetables for meeting each of the elements of the plan, descriptions of the criteria the State will use to measure performance and the process used to develop such criteria, and a description of which official is to be held responsible for ensuring that each performance goal is met.

(9) A description of the uniform, nondiscriminatory State-based administrative complaint procedures in effect under section 402.

(10) If the State received any payment under title I, a description of how such payment will affect the activities proposed to be carried out under the plan, including the amount of funds available for such activities.

(11) How the State will conduct ongoing management of the plan, except that the State may not make any material change in the administration of the plan unless notice of the change—

(A) is developed and published in the Federal Register in accordance with section 255 in the same manner as the State plan;

(B) is subject to public notice and comment in accordance with section 256 in the same manner as the State plan; and

(C) takes effect only after the expiration of the 30-day period which begins on the date notice of the change is published in the Federal Register in accordance with subparagraph (A).

(12) In the case of a State with a State plan in effect under this subtitle during the previous fiscal year, a description of how the plan reflects changes from the State plan for the previous fiscal year and of how the State succeeded in carrying out the State plan for such previous fiscal year.

(13) A description of the committee which participated in the development of the State plan in accordance with section 255

and the procedures followed by the committee under such section and section 256.

(14) How the State will comply with the provisions and requirements of and amendments made by the Military and Overseas Voter Empowerment Act.

(b) REQUIREMENTS FOR ELECTION FUND.—

(1) ELECTION FUND DESCRIBED.—For purposes of subsection (a)(5), a fund described in this subsection with respect to a State is a fund which is established in the treasury of the State government, which is used in accordance with paragraph (2), and which consists of the following amounts:

(A) Amounts appropriated or otherwise made available by the State for carrying out the activities for which the requirements payment is made to the State under this part.

(B) The requirements payment made to the State under this part.

(C) Such other amounts as may be appropriated under law.

(D) Interest earned on deposits of the fund.

(2) USE OF FUND.—Amounts in the fund shall be used by the State exclusively to carry out the activities for which the requirements payment is made to the State under this part.

(3) TREATMENT OF STATES THAT REQUIRE CHANGES TO STATE LAW.—In the case of a State that requires State legislation to establish the fund described in this subsection, the Commission shall defer disbursement of the requirements payment to such State until such time as legislation establishing the fund is enacted.

(c) PROTECTION AGAINST ACTIONS BASED ON INFORMATION IN PLAN.—

(1) IN GENERAL.—No action may be brought under this Act against a State or other jurisdiction on the basis of any information contained in the State plan filed under this part.

(2) EXCEPTION FOR CRIMINAL ACTS.—Paragraph (1) may not be construed to limit the liability of a State or other jurisdiction for criminal acts or omissions.

**SEC. 255. PROCESS FOR DEVELOPMENT AND FILING OF PLAN; PUBLICATION BY COMMISSION.**

(a) IN GENERAL.—The chief State election official shall develop the State plan under this subtitle through a committee of appropriate individuals, including the chief election officials of the two most populous jurisdictions within the States, other local election officials, stake holders (including representatives of groups of individuals with disabilities), and other citizens, appointed for such purpose by the chief State election official.

(b) GEOGRAPHIC REPRESENTATION.—*The members of the committee shall be a representative group of individuals from the State's counties, cities, towns, and Indian tribes, and shall represent the needs of rural as well as urban areas of the State, as the case may be.*

[(b)] (c) PUBLICATION OF PLAN BY COMMISSION.—After receiving the State plan of a State under this subtitle, the Commission shall

cause to have the plan posted on the Commission's website with a notice published in the Federal Register.

\* \* \* \* \*

## **PART 5—PROTECTION AND ADVOCACY SYSTEMS**

\* \* \* \* \*

### **SEC. 292. AUTHORIZATION OF APPROPRIATIONS.**

(a) **IN GENERAL.**—In addition to any other amounts authorized to be appropriated under this subtitle, there are authorized to be appropriated \$10,000,000 for each of the fiscal years 2003, 2004, 2005, and 2006, and for each subsequent fiscal year such sums as may be necessary, for the purpose of making payments under section 291(a) [; except that none of the funds provided by this subsection shall be used to initiate or otherwise participate in any litigation related to election-related disability access, notwithstanding the general authorities that the protection and advocacy systems are otherwise afforded under subtitle C of title I of the Developmental Disabilities Assistance and Bill of Rights Act of 2000 (42 U.S.C. 15041 et seq.)].

(b) **AVAILABILITY.**—Any amounts appropriated pursuant to the authority of this section shall remain available until expended.

\* \* \* \* \*

## **PART 7—GRANTS FOR OBTAINING COMPLIANT PAPER BALLOT VOTING SYSTEMS AND CARRYING OUT VOTING SYSTEM SECURITY IMPROVEMENTS**

### **SEC. 297. GRANTS FOR OBTAINING COMPLIANT PAPER BALLOT VOTING SYSTEMS AND CARRYING OUT VOTING SYSTEM SECURITY IMPROVEMENTS.**

(a) **AVAILABILITY AND USE OF GRANT.**—*The Commission shall make a grant to each eligible State—*

*(1) to replace a voting system—*

*(A) which does not meet the requirements which are first imposed on the State pursuant to the amendments made by the Voter Confidence and Increased Accessibility Act of 2019 with a voting system which does meet such requirements, for use in the regularly scheduled general elections for Federal office held in November 2020, or*

*(B) which does meet such requirements but which is not in compliance with the most recent voluntary voting system guidelines issued by the Commission prior to the regularly scheduled general election for Federal office held in November 2020 with another system which does meet such requirements and is in compliance with such guidelines;*

*(2) to carry out voting system security improvements described in section 297A with respect to the regularly scheduled general elections for Federal office held in November 2020 and each succeeding election for Federal office; and*

(3) to implement and model best practices for ballot design, ballot instructions, and the testing of ballots.

(b) *AMOUNT OF GRANT.*—The amount of a grant made to a State under this section shall be such amount as the Commission determines to be appropriate, except that such amount may not be less than the product of \$1 and the average of the number of individuals who cast votes in any of the two most recent regularly scheduled general elections for Federal office held in the State.

(c) *PRO RATA REDUCTIONS.*—If the amount of funds appropriated for grants under this part is insufficient to ensure that each State receives the amount of the grant calculated under subsection (b), the Commission shall make such pro rata reductions in such amounts as may be necessary to ensure that the entire amount appropriated under this part is distributed to the States.

(d) *SURPLUS APPROPRIATIONS.*—If the amount of funds appropriated for grants authorized under section 297D(a)(2) exceed the amount necessary to meet the requirements of subsection (b), the Commission shall consider the following in making a determination to award remaining funds to a State:

(1) The record of the State in carrying out the following with respect to the administration of elections for Federal office:

(A) Providing voting machines that are less than 10 years old.

(B) Implementing strong chain of custody procedures for the physical security of voting equipment and paper records at all stages of the process.

(C) Conducting pre-election testing on every voting machine and ensuring that paper ballots are available wherever electronic machines are used.

(D) Maintaining offline backups of voter registration lists.

(E) Providing a secure voter registration database that logs requests submitted to the database.

(F) Publishing and enforcing a policy detailing use limitations and security safeguards to protect the personal information of voters in the voter registration process.

(G) Providing secure processes and procedures for reporting vote tallies.

(H) Providing a secure platform for disseminating vote totals.

(2) Evidence of established conditions of innovation and reform in providing voting system security and the proposed plan of the State for implementing additional conditions.

(3) Evidence of collaboration between relevant stakeholders, including local election officials, in developing the grant implementation plan described in section 297B.

(4) The plan of the State to conduct a rigorous evaluation of the effectiveness of the activities carried out with the grant.

(e) *ABILITY OF REPLACEMENT SYSTEMS TO ADMINISTER RANKED CHOICE ELECTIONS.*—To the greatest extent practicable, an eligible State which receives a grant to replace a voting system under this section shall ensure that the replacement system is capable of administering a system of ranked choice voting under which each voter shall rank the candidates for the office in the order of the voter's preference.

**SEC. 297A. VOTING SYSTEM SECURITY IMPROVEMENTS DESCRIBED.**

(a) *PERMITTED USES.*—A voting system security improvement described in this section is any of the following:

(1) *The acquisition of goods and services from qualified election infrastructure vendors by purchase, lease, or such other arrangements as may be appropriate.*

(2) *Cyber and risk mitigation training.*

(3) *A security risk and vulnerability assessment of the State's election infrastructure which is carried out by a provider of cybersecurity services under a contract entered into between the chief State election official and the provider.*

(4) *The maintenance of election infrastructure, including addressing risks and vulnerabilities which are identified under either of the security risk and vulnerability assessments described in paragraph (3), except that none of the funds provided under this part may be used to renovate or replace a building or facility which is used primarily for purposes other than the administration of elections for public office.*

(5) *Providing increased technical support for any information technology infrastructure that the chief State election official deems to be part of the State's election infrastructure or designates as critical to the operation of the State's election infrastructure.*

(6) *Enhancing the cybersecurity and operations of the information technology infrastructure described in paragraph (4).*

(7) *Enhancing the cybersecurity of voter registration systems.*

(b) *QUALIFIED ELECTION INFRASTRUCTURE VENDORS DESCRIBED.*—

(1) *IN GENERAL.*—For purposes of this part, a “qualified election infrastructure vendor” is any person who provides, supports, or maintains, or who seeks to provide, support, or maintain, election infrastructure on behalf of a State, unit of local government, or election agency, who meets the criteria described in paragraph (2).

(2) *CRITERIA.*—The criteria described in this paragraph are such criteria as the Chairman, in coordination with the Secretary of Homeland Security, shall establish and publish, and shall include each of the following requirements:

(A) *The vendor must be owned and controlled by a citizen or permanent resident of the United States.*

(B) *The vendor must disclose to the Chairman and the Secretary, and to the chief State election official of any State to which the vendor provides any goods and services with funds provided under this part, of any sourcing outside the United States for parts of the election infrastructure.*

(C) *The vendor agrees to ensure that the election infrastructure will be developed and maintained in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee.*

(D) *The vendor agrees to maintain its information technology infrastructure in a manner that is consistent with the cybersecurity best practices issued by the Technical Guidelines Development Committee.*

(E) *The vendor agrees to meet the requirements of paragraph (3) with respect to any known or suspected cybersecurity incidents involving any of the goods and services provided by the vendor pursuant to a grant under this part.*

(F) *The vendor agrees to permit independent security testing by the Commission (in accordance with section 231(a)) and by the Secretary of the goods and services provided by the vendor pursuant to a grant under this part.*

**(3) CYBERSECURITY INCIDENT REPORTING REQUIREMENTS.—**

(A) *IN GENERAL.—A vendor meets the requirements of this paragraph if, upon becoming aware of the possibility that an election cybersecurity incident has occurred involving any of the goods and services provided by the vendor pursuant to a grant under this part—*

*(i) the vendor promptly assesses whether or not such an incident occurred, and submits a notification meeting the requirements of subparagraph (B) to the Secretary and the Chairman of the assessment as soon as practicable (but in no case later than 3 days after the vendor first becomes aware of the possibility that the incident occurred);*

*(ii) if the incident involves goods or services provided to an election agency, the vendor submits a notification meeting the requirements of subparagraph (B) to the agency as soon as practicable (but in no case later than 3 days after the vendor first becomes aware of the possibility that the incident occurred), and cooperates with the agency in providing any other necessary notifications relating to the incident; and*

*(iii) the vendor provides all necessary updates to any notification submitted under clause (i) or clause (ii).*

(B) *CONTENTS OF NOTIFICATIONS.—Each notification submitted under clause (i) or clause (ii) of subparagraph (A) shall contain the following information with respect to any election cybersecurity incident covered by the notification:*

*(i) The date, time, and time zone when the election cybersecurity incident began, if known.*

*(ii) The date, time, and time zone when the election cybersecurity incident was detected.*

*(iii) The date, time, and duration of the election cybersecurity incident.*

*(iv) The circumstances of the election cybersecurity incident, including the specific election infrastructure systems believed to have been accessed and information acquired, if any.*

*(v) Any planned and implemented technical measures to respond to and recover from the incident.*

*(vi) In the case of any notification which is an update to a prior notification, any additional material information relating to the incident, including technical data, as it becomes available.*

**SEC. 297B. ELIGIBILITY OF STATES.**

*A State is eligible to receive a grant under this part if the State submits to the Commission, at such time and in such form as the Commission may require, an application containing—*

(1) a description of how the State will use the grant to carry out the activities authorized under this part;

(2) a certification and assurance that, not later than 5 years after receiving the grant, the State will carry out voting system security improvements, as described in section 297A; and

(3) such other information and assurances as the Commission may require.

**SEC. 297C. REPORTS TO CONGRESS.**

Not later than 90 days after the end of each fiscal year, the Commission shall submit a report to the appropriate congressional committees, including the Committees on Homeland Security, House Administration, and the Judiciary of the House of Representatives and the Committees on Homeland Security and Governmental Affairs, the Judiciary, and Rules and Administration of the Senate, on the activities carried out with the funds provided under this part.

**SEC. 297D. AUTHORIZATION OF APPROPRIATIONS.**

(a) **AUTHORIZATION.**—There are authorized to be appropriated for grants under this part—

(1) \$600,000,000 for fiscal year 2019; and

(2) \$175,000,000 for each of the fiscal years 2020, 2022, 2024, and 2026.

(b) **CONTINUING AVAILABILITY OF AMOUNTS.**—Any amounts appropriated pursuant to the authorization of this section shall remain available until expended.

**PART 8—FUNDING FOR POST-ELECTION RISK-LIMITING AUDITS**

**SEC. 298. PAYMENTS FOR POST-ELECTION RISK-LIMITING AUDITS.**

(a) **IN GENERAL.**—The Commission shall pay to States the amount of eligible post-election audit costs.

(b) **ELIGIBLE POST-ELECTION AUDIT COSTS.**—For purposes of this section, the term “eligible post-election audit costs” means, with respect to any State, costs paid or incurred by the State or local government within the State for—

(1) the conduct of any risk-limiting audit (as defined in section 303A) with respect to an election for Federal office occurring after the date of the enactment of this part; and

(2) any equipment, software, or services necessary for the conduct of any such risk-limiting audit.

(c) **SPECIAL RULES.**—

(1) **RULES AND PROCEDURES.**—The Commission shall establish rules and procedures for submission of eligible post-election audit costs for payments under this section.

(2) **INSUFFICIENT FUNDS.**—In any case in which the amounts appropriated under subsection (d) are insufficient to pay all eligible post-election audit costs submitted by States with respect to any Federal election, the amount of such costs paid under subsection (a) to any State shall be equal to the amount that bears the same ratio to the amount which would be paid to such State (determined without regard to this paragraph) as—

(A) the number of individuals who voted in such Federal election in such State; bears to

(B) the total number of individuals who voted in such Federal election in all States submitting a claim for eligible post-election audit costs.

(d) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There is hereby authorized to be appropriated to the Commission such sums as are necessary to carry out this part.

(2) AVAILABILITY.—Any amounts appropriated pursuant to paragraph (1) shall remain available without fiscal year limitation until expended.

## TITLE III—UNIFORM AND NONDISCRIMINATORY ELECTION TECHNOLOGY AND ADMINISTRATION REQUIREMENTS

### Subtitle A—Requirements

#### SEC. 301. VOTING SYSTEMS STANDARDS.

(a) REQUIREMENTS.—Each voting system used in an election for Federal office shall meet the following requirements:

(1) IN GENERAL.—

(A) Except as provided in subparagraph (B), the voting system (including any lever voting system, optical scanning voting system, or direct recording electronic system) shall—

(i) permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and **counted** counted, in accordance with paragraphs (2) and (3);

(ii) provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and **counted** counted, in accordance with paragraphs (2) and (3) (including the opportunity to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error); and

(iii) if the voter selects votes for more than one candidate for a single office—

(I) notify the voter that the voter has selected more than one candidate for a single office on the ballot;

(II) notify the voter before the ballot is cast and **counted** counted, in accordance with paragraphs (2) and (3) of the effect of casting multiple votes for the office; and

(III) provide the voter with the opportunity to correct the ballot before the ballot is cast and **counted** counted, in accordance with paragraphs (2) and (3).

(B) A State or jurisdiction that uses a paper ballot voting system, a punch card voting system, or a central count vot-

ing system (including mail-in absentee ballots and mail-in ballots), may meet the requirements of subparagraph (A)(iii) by—

(i) establishing a voter education program specific to that voting system that notifies each voter of the effect of casting multiple votes for an office; and

(ii) providing the voter with instructions on how to correct the ballot before it is cast and **counted** *counted, in accordance with paragraphs (2) and (3)* (including instructions on how to correct the error through the issuance of a replacement ballot if the voter was otherwise unable to change the ballot or correct any error).

(C) The voting system shall ensure that any notification required under this paragraph preserves the privacy of the voter and the confidentiality of the ballot.

**[(2) AUDIT CAPACITY.—**

**[(A) IN GENERAL.—**The voting system shall produce a record with an audit capacity for such system.

**[(B) MANUAL AUDIT CAPACITY.—**

**[(i)** The voting system shall produce a permanent paper record with a manual audit capacity for such system.

**[(ii)** The voting system shall provide the voter with an opportunity to change the ballot or correct any error before the permanent paper record is produced.

**[(iii)** The paper record produced under subparagraph (A) shall be available as an official record for any recount conducted with respect to any election in which the system is used.]

**(2) PAPER BALLOT REQUIREMENT.—**

**(A) VOTER-VERIFIED PAPER BALLOTS.—**

*(i) PAPER BALLOT REQUIREMENT.—(I) The voting system shall require the use of an individual, durable, voter-verified paper ballot of the voter’s vote that shall be marked and made available for inspection and verification by the voter before the voter’s vote is cast and counted, and which shall be counted by hand or read by an optical character recognition device or other counting device. For purposes of this subclause, the term “individual, durable, voter-verified paper ballot” means a paper ballot marked by the voter by hand or a paper ballot marked through the use of a nontabulating ballot marking device or system, so long as the voter shall have the option to mark his or her ballot by hand.*

*(II) The voting system shall provide the voter with an opportunity to correct any error on the paper ballot before the permanent voter-verified paper ballot is preserved in accordance with clause (i).*

*(III) The voting system shall not preserve the voter-verified paper ballots in any manner that makes it possible, at any time after the ballot has been cast, to associate a voter with the record of the voter’s vote without the voter’s consent.*

(ii) *PRESERVATION AS OFFICIAL RECORD.*—The individual, durable, voter-verified paper ballot used in accordance with clause (i) shall constitute the official ballot and shall be preserved and used as the official ballot for purposes of any recount or audit conducted with respect to any election for Federal office in which the voting system is used.

(iii) *MANUAL COUNTING REQUIREMENTS FOR RECOUNTS AND AUDITS.*—(I) Each paper ballot used pursuant to clause (i) shall be suitable for a manual audit, and shall be counted by hand in any recount or audit conducted with respect to any election for Federal office.

(II) In the event of any inconsistencies or irregularities between any electronic vote tallies and the vote tallies determined by counting by hand the individual, durable, voter-verified paper ballots used pursuant to clause (i), and subject to subparagraph (B), the individual, durable, voter-verified paper ballots shall be the true and correct record of the votes cast.

(iv) *APPLICATION TO ALL BALLOTS.*—The requirements of this subparagraph shall apply to all ballots cast in elections for Federal office, including ballots cast by absent uniformed services voters and overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act and other absentee voters.

(B) *SPECIAL RULE FOR TREATMENT OF DISPUTES WHEN PAPER BALLOTS HAVE BEEN SHOWN TO BE COMPROMISED.*—

(i) *IN GENERAL.*—In the event that—

(I) there is any inconsistency between any electronic vote tallies and the vote tallies determined by counting by hand the individual, durable, voter-verified paper ballots used pursuant to subparagraph (A)(i) with respect to any election for Federal office; and

(II) it is demonstrated by clear and convincing evidence (as determined in accordance with the applicable standards in the jurisdiction involved) in any recount, audit, or contest of the result of the election that the paper ballots have been compromised (by damage or mischief or otherwise) and that a sufficient number of the ballots have been so compromised that the result of the election could be changed,

the determination of the appropriate remedy with respect to the election shall be made in accordance with applicable State law, except that the electronic tally shall not be used as the exclusive basis for determining the official certified result.

(ii) *RULE FOR CONSIDERATION OF BALLOTS ASSOCIATED WITH EACH VOTING MACHINE.*—For purposes of clause (i), only the paper ballots deemed compromised, if any, shall be considered in the calculation of whether or not the result of the election could be changed due to the compromised paper ballots.

(3) ACCESSIBILITY FOR INDIVIDUALS WITH DISABILITIES.—The voting system shall—

(A) be accessible for individuals with disabilities, including nonvisual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters;

[(B) satisfy the requirement of subparagraph (A) through the use of at least one direct recording electronic voting system or other voting system equipped for individuals with disabilities at each polling place; and]

*(B)(i) satisfy the requirement of subparagraph (A) through the use of at least 1 voting system at each polling place that—*

*(I) is equipped for individuals with disabilities, including nonvisual and enhanced visual accessibility for the blind and visually impaired, and contains features to support enhanced manual accessibility for the mobility and dexterity impaired;*

*(II) in the case of any election for Federal office occurring after the date that is 6 years after the date of the enactment of the Securing America's Federal Elections Act—*

*(aa) marks ballots that are identical in size, ink, and paper stock to those ballots that would be marked by hand or a ballot marking device used by voters who do not have accessibility needs;*

*(bb) marks the ballot in such a way that someone examining the ballot will not be able to readily determine whether the ballot was marked by hand or machine; and*

*(cc) combines ballots produced by the voting system with ballots marked by voters using other types of voting systems used by the State or jurisdiction in a way that prevents identification of which ballots were cast using each voting system; and*

*(III) is made available for use by any voter who requests to use it; and*

*(ii) in the case of any election for Federal office occurring after the date that is 6 years after the date of the enactment of the Securing America's Federal Elections Act, meet the requirements of subparagraph (A) and paragraph (2)(A) by using a system that allows the voter to privately and independently verify the accuracy of the permanent paper ballot through the presentation, in accessible form, of the printed or marked vote selections from the same printed or marked information that would be used for any vote tabulation or auditing; and*

(C) if purchased with funds made available under title II on or after January 1, 2007, meet the voting system standards for disability access (as outlined in this paragraph).

*Nothing in subparagraph (B) shall be construed to prohibit the use of an accessible ballot that may be printed or marked by the voter at home.*

(4) **ALTERNATIVE LANGUAGE ACCESSIBILITY.**—The voting system (including the paper ballots required to be used under paragraph (2)) shall provide alternative language accessibility pursuant to the requirements of section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a).

(5) **ERROR RATES.**—The error rate of the voting system in counting ballots (determined by taking into account only those errors which are attributable to the voting system and not attributable to an act of the voter) shall comply with the error rate standards established under section 3.2.1 of the voting systems standards issued by the Federal Election Commission which are in effect on the date of the enactment of this Act.

(6) **UNIFORM DEFINITION OF WHAT CONSTITUTES A VOTE.**—Each State shall adopt uniform and nondiscriminatory standards that define what constitutes a vote and what will be counted as a vote for each category of voting system used in the State.

(7) **DURABILITY AND READABILITY REQUIREMENTS FOR BALLOTS.**—

(A) **DURABILITY REQUIREMENTS FOR PAPER BALLOTS.**—

(i) **IN GENERAL.**—All voter-verified paper ballots required to be used under this Act shall be marked or printed on durable paper.

(ii) **DEFINITION.**—For purposes of this Act, paper is “durable” if it is capable of withstanding multiple counts and recounts by hand without compromising the fundamental integrity of the ballots, and capable of retaining the information marked or printed on them for the full duration of a retention and preservation period of 22 months.

(B) **READABILITY REQUIREMENTS FOR PAPER BALLOTS MARKED BY BALLOT MARKING DEVICE.**—All voter-verified paper ballots completed by the voter through the use of a ballot marking device shall be clearly readable by the voter without assistance (other than eyeglasses or other personal vision enhancing devices) and by an optical character recognition device or other device equipped for individuals with disabilities.

(8) **PRINTING REQUIREMENTS FOR BALLOTS.**—All paper ballots used in an election for Federal office shall be printed in the United States on recycled paper manufactured in the United States.

(9) **BALLOT TABULATING METHODS.**—

(A) **IN GENERAL.**—The voting system tabulates ballots by hand or through the use of an optical scanning device that meets the requirements of subparagraph (B).

(B) **REQUIREMENTS FOR OPTICAL SCANNING DEVICES.**—Except as provided in subparagraph (C), the requirements of this subparagraph are as follows:

(i) The device is designed and built in a manner in which it is mechanically impossible for the device to

add or change the vote selections on a printed or marked ballot.

(ii) The device is capable of exporting its data (including vote tally data sets and cast vote records) in a machine-readable, open data standard format required by the Commission, in consultation with the Director of the National Institute of Standards and Technology.

(iii) The device consists of hardware that—

(I) is certified under section 2216 of the Homeland Security Act; and

(II) demonstrably conforms to a hardware component manifest describing point-of-origin information (including upstream hardware supply chain information for each component) that—

(aa) has been provided to the Commission, the Director of Cybersecurity and Infrastructure Security under section 2215 of the Homeland Security Act, and the chief State election official for each State in which the device is used; and

(bb) may be shared by any entity to whom it has been provided under item (aa) with independent experts for cybersecurity analysis.

(iv) The device utilizes technology that prevents the operation of the device if any hardware components do not meet the requirements of clause (iii).

(v) The device operates using software—

(I) for which the source code, system build tools, and compilation parameters—

(aa) have been provided to the Commission, the Director of Cybersecurity and Infrastructure Security under section 2215 of the Homeland Security Act, and the chief State election official for each State in which the device is used; and

(bb) may be shared by any entity to whom it has been provided under item (aa) with independent experts for cybersecurity analysis; and

(II) that is certified under section 2216 of the Homeland Security Act.

(vi) The device utilizes technology that prevents the running of software on the device that does not meet the requirements of clause (v).

(vii) The device utilizes technology that enables election officials, cybersecurity researchers, and voters to verify that the software running on the device—

(I) was built from a specific, untampered version of the code that is described in clause (v); and

(II) uses the system build tools and compilation parameters that are described in clause (v).

(viii) The device contains such other security requirements as the Director of Cybersecurity and Infrastructure Security requires.

(C) WAIVER.—

(i) *IN GENERAL.*—*The Director of Cybersecurity and Infrastructure Security, in consultation with the Director of the National Institute of Standards and Technology, may waive one or more of the requirements of subparagraph (B) (other than the requirement of clause (i) thereof) with respect to any device for a period of not to exceed 2 years.*

(ii) *PUBLICATION.*—*Information relating to any waiver granted under clause (i) shall be made publicly available on the Internet.*

(D) *EFFECTIVE DATE.*—*Each State and jurisdiction shall be required to comply with the requirements of this paragraph for the regularly scheduled election for Federal office in November 2024, and for each subsequent election for Federal office.*

(9) *REQUIRING USE OF SOFTWARE AND HARDWARE FOR WHICH INFORMATION IS DISCLOSED BY MANUFACTURER.*—

(A) *REQUIRING USE OF SOFTWARE FOR WHICH SOURCE CODE IS DISCLOSED BY MANUFACTURER.*—

(i) *IN GENERAL.*—*In the operation of voting systems in an election for Federal office, a State may only use software for which the manufacturer makes the source code (in the form in which will be used at the time of the election) publicly available online under a license that grants a worldwide, royalty-free, non-exclusive, perpetual, sub-licensable license to all intellectual property rights in such source code, except that the manufacturer may prohibit a person who obtains the software from using the software in a manner that is primarily intended for or directed toward commercial advantage or private monetary compensation that is unrelated to carrying out legitimate research or cybersecurity activity.*

(ii) *EXCEPTIONS.*—*Clause (i) does not apply with respect to—*

(I) *widely-used operating system software which is not specific to voting systems and for which the source code or baseline functionality is not altered;*  
or

(II) *widely-used cybersecurity software which is not specific to voting systems and for which the source code or baseline functionality is not altered.*

(B) *REQUIRING USE OF HARDWARE FOR WHICH INFORMATION IS DISCLOSED BY MANUFACTURER.*—

(i) *REQUIRING DISCLOSURE OF HARDWARE.*—*A State may not use a voting system in an election for Federal office unless the manufacturer of the system publicly discloses online the identification of the hardware used to operate the system.*

(ii) *ADDITIONAL DISCLOSURE REQUIREMENTS FOR CUSTOM OR ALTERED HARDWARE.*—*To the extent that the hardware used to operate a voting system or any component thereof is not widely-used, or is widely-used but is altered, the State may not use the system in an election for Federal office unless—*

(I) the manufacturer of the system publicly discloses online the components of the hardware, the design of such components, and how such components are connected in the operation of the system; and

(II) the manufacturer makes the design (in the form which will be used at the time of the election) publicly available online under a license that grants a worldwide, royalty-free, non-exclusive, perpetual, sub-licensable license to all intellectual property rights in the design of the hardware or the component, except that the manufacturer may prohibit a person who obtains the design from using the design in a manner that is primarily intended for or directed toward commercial advantage or private monetary compensation that is unrelated to carrying out legitimate research or cybersecurity activity.

(10) PROHIBITION OF USE OF WIRELESS COMMUNICATIONS DEVICES IN SYSTEMS OR DEVICES.—

(A) IN GENERAL.—No system or device upon which ballot marking devices or optical scanners are configured, upon which ballots are marked by voters (except as necessary for individuals with disabilities to use ballot marking devices that meet the accessibility requirements of paragraph (3)), or upon which votes are cast, tabulated, or aggregated shall contain, use, or be accessible by any wireless, power-line, or concealed communication device.

(B) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this paragraph for the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office.

(11) PROHIBITING CONNECTION OF SYSTEM TO THE INTERNET.—

(A) IN GENERAL.—No system or device upon which ballot marking devices or optical scanners are configured, upon which ballots are marked by voters, or upon which votes are cast, tabulated, or aggregated shall be connected to the Internet or any non-local computer system via telephone or other communication network at any time.

(B) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this paragraph for the regularly scheduled election for Federal office in November 2020, and for each subsequent election for Federal office.

(10) VOTING MACHINE REQUIREMENTS.—By not later than the date of the regularly scheduled general election for Federal office occurring in November 2022, each State shall seek to ensure that any voting machine used in such election and in any subsequent election for Federal office is manufactured in the United States.

(13) BALLOT MARKING DEVICES.—

(A) *IN GENERAL.*—*In the case of a voting system that uses a ballot marking device, the ballot marking device shall be a device that—*

*(i) is not capable of tabulating votes;*

*(ii) except in the case of a ballot marking device used exclusively to comply with the requirements of paragraph (3), is certified in accordance with section 232 as meeting the requirements of subparagraph (B); and*

*(iii) is certified under section 2216 of the Homeland Security Act as meeting the requirements of clauses (iii) through (viii) of section 301(a)(9)(B).*

(B) *REQUIREMENTS.*—

*(i) IN GENERAL.*—*A ballot marking device meets the requirements of this subparagraph if, during a double-masked test conducted by a qualified independent user experience research laboratory (as defined in section 232(b)(4)) of a simulated election scenario which meets the requirements of clause (ii), there is less than a 5 percent chance that an ordinary voter using the device would not detect and report any difference between the vote selection printed on the ballot by the ballot marking device and the vote selection indicated by the voter.*

*(ii) SIMULATED ELECTION SCENARIO.*—*A simulated election scenario meets the requirements of this clause if it is conducted with—*

*(I) a pool of subjects that are—*

*(aa) diverse in age, gender, education, and physical limitations; and*

*(bb) representative of the communities in which the voting system will be used; and*

*(II) ballots that are representative of ballots ordinarily used in the communities in which the voting system will be used.*

(C) *EFFECTIVE DATE.*—*Each State and jurisdiction shall be required to comply with the requirements of this paragraph for the regularly scheduled election for Federal office in November 2022, and for each subsequent election for Federal office.*

(b) *VOTING SYSTEM DEFINED.*—*In [this section] this Act, the term “voting system” means—*

*(1) the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—*

*(A) to define ballots;*

*(B) to cast and count votes;*

*(C) to report or display election results; and*

*(D) to maintain and produce any audit trail information;*

**[and]**

*(2) any electronic poll book used with respect to the election; and*

**[(2)] (3) the practices and associated documentation used—**

**(A) to identify system components and versions of such components;**

(B) to test the system during its development and maintenance;

(C) to maintain records of system errors and defects;

(D) to determine specific system changes to be made to a system after the initial qualification of the system; and

(E) to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

(c) *ELECTRONIC POLL BOOK DEFINED.*—*In this Act, the term “electronic poll book” means the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment) that is used—*

(1) *to retain the list of registered voters at a polling location, or vote center, or other location at which voters cast votes in an election for Federal office; and*

(2) *to identify registered voters who are eligible to vote in an election.*

[(c)] (d) CONSTRUCTION.—

(1) IN GENERAL.—Nothing in this section shall be construed to prohibit a State or jurisdiction which used a particular type of voting system in the elections for Federal office held in November 2000 from using the same type of system after the effective date of this section, so long as the system meets or is modified to meet the requirements of this section.

(2) PROTECTION OF PAPER BALLOT VOTING SYSTEMS.—For purposes of subsection (a)(1)(A)(i), the term “verify” may not be defined in a manner that makes it impossible for a paper ballot voting system to meet the requirements of such subsection or to be modified to meet such requirements.

[(d) EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this section on and after January 1, 2006.]

(e) *EFFECTIVE DATE.*—

(1) IN GENERAL.—*Except as provided in paragraph (2), each State and jurisdiction shall be required to comply with the requirements of this section on and after January 1, 2006.*

(2) SPECIAL RULE FOR CERTAIN REQUIREMENTS.—

(A) IN GENERAL.—*Except as provided in section 105(b) of the Securing America’s Federal Elections Act and subparagraphs (B) and (C), the requirements of this section which are first imposed on a State and jurisdiction pursuant to the amendments made by the Voter Confidence and Increased Accessibility Act of 2019 shall apply with respect to voting systems used for any election for Federal office held in 2020 or any succeeding year.*

(B) DELAY FOR JURISDICTIONS USING CERTAIN PAPER RECORD PRINTERS OR CERTAIN SYSTEMS USING OR PRODUCING VOTER-VERIFIED PAPER RECORDS IN 2018.—

(i) DELAY.—*In the case of a jurisdiction described in clause (ii), subparagraph (A) shall apply to a voting system in the jurisdiction as if the reference in such subparagraph to “2020” were a reference to “2022”, but only with respect to the following requirements of this section:*

(I) Paragraph (2)(A)(i)(I) of subsection (a) (relating to the use of voter-verified paper ballots).

(II) Paragraph (3)(B)(ii)(I) and (II) of subsection (a) (relating to access to verification from and casting of the durable paper ballot).

(III) Paragraph (7) of subsection (a) (relating to durability and readability requirements for ballots).

(ii) JURISDICTIONS DESCRIBED.—A jurisdiction described in this clause is a jurisdiction—

(I) which used voter-verified paper record printers attached to direct recording electronic voting machines, or which used other voting systems that used or produced paper records of the vote verifiable by voters but that are not in compliance with paragraphs (2)(A)(i)(I), (3)(B)(iii)(I) and (II), and (7) of subsection (a) (as amended or added by the Voter Confidence and Increased Accessibility Act of 2019), for the administration of the regularly scheduled general election for Federal office held in November 2018; and

(II) which will continue to use such printers or systems for the administration of elections for Federal office held in years before 2022.

(iii) MANDATORY AVAILABILITY OF PAPER BALLOTS AT POLLING PLACES USING GRANDFATHERED PRINTERS AND SYSTEMS.—

(I) REQUIRING BALLOTS TO BE OFFERED AND PROVIDED.—The appropriate election official at each polling place that uses a printer or system described in clause (ii)(I) for the administration of elections for Federal office shall offer each individual who is eligible to cast a vote in the election at the polling place the opportunity to cast the vote using a blank pre-printed paper ballot which the individual may mark by hand and which is not produced by the direct recording electronic voting machine or other such system. The official shall provide the individual with the ballot and the supplies necessary to mark the ballot, and shall ensure (to the greatest extent practicable) that the waiting period for the individual to cast a vote is the lesser of 30 minutes or the average waiting period for an individual who does not agree to cast the vote using such a paper ballot under this clause.

(II) TREATMENT OF BALLOT.—Any paper ballot which is cast by an individual under this clause shall be counted and otherwise treated as a regular ballot for all purposes (including by incorporating it into the final unofficial vote count (as defined by the State) for the precinct) and not as a provisional ballot, unless the individual casting the ballot would have otherwise been required to cast a provisional ballot.

(III) *POSTING OF NOTICE.*—The appropriate election official shall ensure there is prominently displayed at each polling place a notice that describes the obligation of the official to offer individuals the opportunity to cast votes using a pre-printed blank paper ballot.

(IV) *TRAINING OF ELECTION OFFICIALS.*—The chief State election official shall ensure that election officials at polling places in the State are aware of the requirements of this clause, including the requirement to display a notice under subclause (III), and are aware that it is a violation of the requirements of this title for an election official to fail to offer an individual the opportunity to cast a vote using a blank pre-printed paper ballot.

(V) *PERIOD OF APPLICABILITY.*—The requirements of this clause apply only during the period in which the delay is in effect under clause (i).

(C) *SPECIAL RULE FOR JURISDICTIONS USING CERTAIN NONTABULATING BALLOT MARKING DEVICES.*—In the case of a jurisdiction which uses a nontabulating ballot marking device which automatically deposits the ballot into a privacy sleeve, subparagraph (A) shall apply to a voting system in the jurisdiction as if the reference in such subparagraph to “any election for Federal office held in 2020 or any succeeding year” were a reference to “elections for Federal office occurring held in 2022 or each succeeding year”, but only with respect to paragraph (3)(B)(iii)(II) of subsection (a) (relating to nonmanual casting of the durable paper ballot).

**SEC. 301A. PRE-ELECTION REPORTS ON VOTING SYSTEM USAGE.**

(a) *REQUIRING STATES TO SUBMIT REPORTS.*—Not later than 120 days before the date of each regularly scheduled general election for Federal office, the chief State election official of a State shall submit a report to the Commission containing a detailed voting system usage plan for each jurisdiction in the State which will administer the election, including a detailed plan for the usage of electronic poll books and other equipment and components of such system.

(b) *EFFECTIVE DATE.*—Subsection (a) shall apply with respect to the regularly scheduled general election for Federal office held in November 2020 and each succeeding regularly scheduled general election for Federal office.

\* \* \* \* \*

**SEC. 303. COMPUTERIZED STATEWIDE VOTER REGISTRATION LIST REQUIREMENTS AND REQUIREMENTS FOR VOTERS WHO REGISTER BY MAIL.**

(a) *COMPUTERIZED STATEWIDE VOTER REGISTRATION LIST REQUIREMENTS.*—

(1) *IMPLEMENTATION.*—

(A) *IN GENERAL.*—Except as provided in subparagraph (B), each State, acting through the chief State election official, shall implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined,

maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State (in this subsection referred to as the “computerized list”), and includes the following:

(i) The computerized list shall serve as the single system for storing and managing the official list of registered voters throughout the State.

(ii) The computerized list contains the name and registration information of every legally registered voter in the State.

(iii) Under the computerized list, a unique identifier is assigned to each legally registered voter in the State.

(iv) The computerized list shall be coordinated with other agency databases within the State.

(v) Any election official in the State, including any local election official, may obtain immediate electronic access to the information contained in the computerized list.

(vi) All voter registration information obtained by any local election official in the State shall be electronically entered into the computerized list on an expedited basis at the time the information is provided to the local official.

(vii) The chief State election official shall provide such support as may be required so that local election officials are able to enter information as described in clause (vi).

(viii) The computerized list shall serve as the official voter registration list for the conduct of all elections for Federal office in the State.

(B) EXCEPTION.—The requirement under subparagraph (A) shall not apply to a State in which, under a State law in effect continuously on and after the date of the enactment of this Act, there is no voter registration requirement for individuals in the State with respect to elections for Federal office.

(2) COMPUTERIZED LIST MAINTENANCE.—

(A) IN GENERAL.—The appropriate State or local election official shall perform list maintenance with respect to the computerized list on a regular basis as follows:

(i) If an individual is to be removed from the computerized list, such individual shall be removed in accordance with the provisions of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg et seq.), including subsections (a)(4), (c)(2), (d), and (e) of section 8 of such Act (42 U.S.C. 1973gg-6).

(ii) For purposes of removing names of ineligible voters from the official list of eligible voters—

(I) under section 8(a)(3)(B) of such Act (42 U.S.C. 1973gg-6(a)(3)(B)), the State shall coordinate the computerized list with State agency records on felony status; and

(II) by reason of the death of the registrant under section 8(a)(4)(A) of such Act (42 U.S.C. 1973gg-6(a)(4)(A)), the State shall coordinate the computerized list with State agency records on death.

(iii) Notwithstanding the preceding provisions of this subparagraph, if a State is described in section 4(b) of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-2(b)), that State shall remove the names of ineligible voters from the computerized list in accordance with State law.

(B) CONDUCT.—The list maintenance performed under subparagraph (A) shall be conducted in a manner that ensures that—

(i) the name of each registered voter appears in the computerized list;

(ii) only voters who are not registered or who are not eligible to vote are removed from the computerized list; and

(iii) duplicate names are eliminated from the computerized list.

(3) TECHNOLOGICAL SECURITY OF COMPUTERIZED LIST.—The appropriate State or local official shall provide adequate technological security measures to prevent the unauthorized access to the computerized list established under this section[.], *as well as other measures to prevent and deter cybersecurity incidents, as identified by the Commission, the Secretary of Homeland Security, and the Technical Guidelines Development Committee.*

(4) MINIMUM STANDARD FOR ACCURACY OF STATE VOTER REGISTRATION RECORDS.—The State election system shall include provisions to ensure that voter registration records in the State are accurate and are updated regularly, including the following:

(A) A system of file maintenance that makes a reasonable effort to remove registrants who are ineligible to vote from the official list of eligible voters. Under such system, consistent with the National Voter Registration Act of 1993 (42 U.S.C. 1973gg et seq.), registrants who have not responded to a notice and who have not voted in 2 consecutive general elections for Federal office shall be removed from the official list of eligible voters, except that no registrant may be removed solely by reason of a failure to vote.

(B) Safeguards to ensure that eligible voters are not removed in error from the official list of eligible voters.

(5) VERIFICATION OF VOTER REGISTRATION INFORMATION.—

(A) REQUIRING PROVISION OF CERTAIN INFORMATION BY APPLICANTS.—

(i) IN GENERAL.—Except as provided in clause (ii), notwithstanding any other provision of law, an application for voter registration for an election for Federal office may not be accepted or processed by a State unless the application includes—

(I) in the case of an applicant who has been issued a current and valid driver's license, the applicant's driver's license number; or

(II) in the case of any other applicant (other than an applicant to whom clause (i) applies), the last 4 digits of the applicant's social security number.

(ii) SPECIAL RULE FOR APPLICANTS WITHOUT DRIVER'S LICENSE OR SOCIAL SECURITY NUMBER.—If an applicant for voter registration for an election for Federal office has not been issued a current and valid driver's license or a social security number, the State shall assign the applicant a number which will serve to identify the applicant for voter registration purposes. To the extent that the State has a computerized list in effect under this subsection and the list assigns unique identifying numbers to registrants, the number assigned under this clause shall be the unique identifying number assigned under the list.

(iii) DETERMINATION OF VALIDITY OF NUMBERS PROVIDED.—The State shall determine whether the information provided by an individual is sufficient to meet the requirements of this subparagraph, in accordance with State law.

(B) REQUIREMENTS FOR STATE OFFICIALS.—

(i) SHARING INFORMATION IN DATABASES.—The chief State election official and the official responsible for the State motor vehicle authority of a State shall enter into an agreement to match information in the database of the statewide voter registration system with information in the database of the motor vehicle authority to the extent required to enable each such official to verify the accuracy of the information provided on applications for voter registration.

(ii) AGREEMENTS WITH COMMISSIONER OF SOCIAL SECURITY.—The official responsible for the State motor vehicle authority shall enter into an agreement with the Commissioner of Social Security under section 205(r)(8) of the Social Security Act (as added by subparagraph (C)).

(C) ACCESS TO FEDERAL INFORMATION.—Section 205(r) of the Social Security Act (42 U.S.C. 405(r)) is amended by adding at the end the following new paragraph:

“(8)(A) The Commissioner of Social Security shall, upon the request of the official responsible for a State driver's license agency pursuant to the Help America Vote Act of 2002—

“(i) enter into an agreement with such official for the purpose of verifying applicable information, so long as the requirements of subparagraphs (A) and (B) of paragraph (3) are met; and

“(ii) include in such agreement safeguards to assure the maintenance of the confidentiality of any applicable information disclosed and procedures to permit such agency to use the applicable information for the purpose of maintaining its records.

“(B) Information provided pursuant to an agreement under this paragraph shall be provided at such time, in such place, and in such manner as the Commissioner determines appropriate.

“(C) The Commissioner shall develop methods to verify the accuracy of information provided by the agency with respect to applications for voter registration, for whom the last 4 digits of a social security number are provided instead of a driver’s license number.

“(D) For purposes of this paragraph—

“(i) the term ‘applicable information’ means information regarding whether—

“(I) the name (including the first name and any family forename or surname), the date of birth (including the month, day, and year), and social security number of an individual provided to the Commissioner match the information contained in the Commissioner’s records, and

“(II) such individual is shown on the records of the Commissioner as being deceased; and

“(ii) the term ‘State driver’s license agency’ means the State agency which issues driver’s licenses to individuals within the State and maintains records relating to such licensure.

“(E) Nothing in this paragraph may be construed to require the provision of applicable information with regard to a request for a record of an individual if the Commissioner determines there are exceptional circumstances warranting an exception (such as safety of the individual or interference with an investigation).

“(F) Applicable information provided by the Commission pursuant to an agreement under this paragraph or by an individual to any agency that has entered into an agreement under this paragraph shall be considered as strictly confidential and shall be used only for the purposes described in this paragraph and for carrying out an agreement under this paragraph. Any officer or employee or former officer or employee of a State, or any officer or employee or former officer or employee of a contractor of a State who, without the written authority of the Commissioner, publishes or communicates any applicable information in such individual’s possession by reason of such employment or position as such an officer, shall be guilty of a felony and upon conviction thereof shall be fined or imprisoned, or both, as described in section 208.”

(D) SPECIAL RULE FOR CERTAIN STATES.—In the case of a State which is permitted to use social security numbers, and provides for the use of social security numbers, on applications for voter registration, in accordance with section 7 of the Privacy Act of 1974 (5 U.S.C. 552a note), the provisions of this paragraph shall be optional.

(b) REQUIREMENTS FOR VOTERS WHO REGISTER BY MAIL.—

(1) IN GENERAL.—Notwithstanding section 6(c) of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4(c)) and subject to paragraph (3), a State shall, in a uniform and

nondiscriminatory manner, require an individual to meet the requirements of paragraph (2) if—

- (A) the individual registered to vote in a jurisdiction by mail; and
- (B)(i) the individual has not previously voted in an election for Federal office in the State; or
- (ii) the individual has not previously voted in such an election in the jurisdiction and the jurisdiction is located in a State that does not have a computerized list that complies with the requirements of subsection (a).

(2) REQUIREMENTS.—

(A) IN GENERAL.—An individual meets the requirements of this paragraph if the individual—

- (i) in the case of an individual who votes in person—
  - (I) presents to the appropriate State or local election official a current and valid photo identification; or
  - (II) presents to the appropriate State or local election official a copy of a current utility bill, bank statement, government check, paycheck, or other government document that shows the name and address of the voter; or
- (ii) in the case of an individual who votes by mail, submits with the ballot—
  - (I) a copy of a current and valid photo identification; or
  - (II) a copy of a current utility bill, bank statement, government check, paycheck, or other government document that shows the name and address of the voter.

(B) FAIL-SAFE VOTING.—

- (i) IN PERSON.—An individual who desires to vote in person, but who does not meet the requirements of subparagraph (A)(i), may cast a provisional ballot under section 302(a).
- (ii) BY MAIL.—An individual who desires to vote by mail but who does not meet the requirements of subparagraph (A)(ii) may cast such a ballot by mail and the ballot shall be counted as a provisional ballot in accordance with section 302(a).

(3) INAPPLICABILITY.—Paragraph (1) shall not apply in the case of a person—

(A) who registers to vote by mail under section 6 of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4) and submits as part of such registration either—

- (i) a copy of a current and valid photo identification;
- or
- (ii) a copy of a current utility bill, bank statement, government check, paycheck, or government document that shows the name and address of the voter;

(B)(i) who registers to vote by mail under section 6 of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4) and submits with such registration either—

- (I) a driver's license number; or

(II) at least the last 4 digits of the individual's social security number; and

(ii) with respect to whom a State or local election official matches the information submitted under clause (i) with an existing State identification record bearing the same number, name and date of birth as provided in such registration; or

(C) who is—

(i) entitled to vote by absentee ballot under the Uniformed and Overseas Citizens Absentee Voting Act (42 U.S.C. 1973ff-1 et seq.);

(ii) provided the right to vote otherwise than in person under section 3(b)(2)(B)(ii) of the Voting Accessibility for the Elderly and Handicapped Act (42 U.S.C. 1973ee-1(b)(2)(B)(ii)); or

(iii) entitled to vote otherwise than in person under any other Federal law.

(4) CONTENTS OF MAIL-IN REGISTRATION FORM.—

(A) IN GENERAL.—The mail voter registration form developed under section 6 of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg-4) shall include the following:

(i) The question “Are you a citizen of the United States of America?” and boxes for the applicant to check to indicate whether the applicant is or is not a citizen of the United States.

(ii) The question “Will you be 18 years of age on or before election day?” and boxes for the applicant to check to indicate whether or not the applicant will be 18 years of age or older on election day.

(iii) The statement “If you checked ‘no’ in response to either of these questions, do not complete this form.”.

(iv) A statement informing the individual that if the form is submitted by mail and the individual is registering for the first time, the appropriate information required under this section must be submitted with the mail-in registration form in order to avoid the additional identification requirements upon voting for the first time.

(B) INCOMPLETE FORMS.—If an applicant for voter registration fails to answer the question included on the mail voter registration form pursuant to subparagraph (A)(i), the registrar shall notify the applicant of the failure and provide the applicant with an opportunity to complete the form in a timely manner to allow for the completion of the registration form prior to the next election for Federal office (subject to State law).

(5) CONSTRUCTION.—Nothing in this subsection shall be construed to require a State that was not required to comply with a provision of the National Voter Registration Act of 1993 (42 U.S.C. 1973gg et seq.) before the date of the enactment of this Act to comply with such a provision after such date.

(c) PERMITTED USE OF LAST 4 DIGITS OF SOCIAL SECURITY NUMBERS.—The last 4 digits of a social security number described in subsections (a)(5)(A)(i)(II) and (b)(3)(B)(i)(II) shall not be considered

to be a social security number for purposes of section 7 of the Privacy Act of 1974 (5 U.S.C. 552a note).

(d) EFFECTIVE DATE.—

(1) COMPUTERIZED STATEWIDE VOTER REGISTRATION LIST REQUIREMENTS.—

(A) IN GENERAL.—Except as provided in subparagraph (B), each State and jurisdiction shall be required to comply with the requirements of subsection (a) on and after January 1, 2004.

(B) WAIVER.—If a State or jurisdiction certifies to the Commission not later than January 1, 2004, that the State or jurisdiction will not meet the deadline described in subparagraph (A) for good cause and includes in the certification the reasons for the failure to meet such deadline, subparagraph (A) shall apply to the State or jurisdiction as if the reference in such subparagraph to “January 1, 2004” were a reference to “January 1, 2006”.

(2) REQUIREMENT FOR VOTERS WHO REGISTER BY MAIL.—

(A) IN GENERAL.—Each State and jurisdiction shall be required to comply with the requirements of subsection (b) on and after January 1, 2004, and shall be prepared to receive registration materials submitted by individuals described in subparagraph (B) on and after the date described in such subparagraph.

(B) APPLICABILITY WITH RESPECT TO INDIVIDUALS.—The provisions of subsection (b) shall apply to any individual who registers to vote on or after January 1, 2003.

**SEC. 303A. RISK-LIMITING AUDITS.**

(a) DEFINITIONS.—*In this section:*

(1) *RISK-LIMITING AUDIT.*—*The term “risk-limiting audit” means, with respect to any election contest, a post-election process that—*

*(A) has a probability of at least 95 percent of correcting the reported outcome if the reported outcome is not the correct outcome;*

*(B) will not change the outcome if the reported outcome is the correct outcome; and*

*(C) involves a manual adjudication of voter intent from some or all of the ballots validly cast in the election contest.*

(2) *REPORTED OUTCOME; CORRECT OUTCOME; OUTCOME.*—

*(A) REPORTED OUTCOME.*—*The term “reported outcome” means the outcome of an election contest which is determined according to the canvass and which will become the official, certified outcome unless it is revised by an audit, recount, or other legal process.*

*(B) CORRECT OUTCOME.*—*The term “correct outcome” means the outcome that would be determined by a manual adjudication of voter intent for all votes validly cast in the election contest.*

*(C) OUTCOME.*—*The term “outcome” means the winner or set of winners of an election contest.*

(3) *MANUAL ADJUDICATION OF VOTER INTENT.*—*The term “manual adjudication of voter intent” means direct inspection and determination by humans, without assistance from elec-*

tronic or mechanical tabulation devices, of the ballot choices marked by voters on each voter-verified paper record.

(4) **BALLOT MANIFEST.**—The term “ballot manifest” means a record maintained by each jurisdiction that—

(A) is created without reliance on any part of the voting system used to tabulate votes;

(B) functions as a sampling frame for conducting a risk-limiting audit; and

(C) accounts for all ballots validly cast regardless of how or whether they were tabulated and includes a precise description of the manner in which the ballots are physically stored, including the total number of physical groups of ballots, the numbering system for each group, a unique label for each group, and the number of ballots in each such group.

(b) **REQUIREMENTS.**—

(1) **IN GENERAL.**—

(A) **AUDITS.**—

(i) **IN GENERAL.**—Each State and jurisdiction shall administer risk-limiting audits of the results of all election contests for Federal office held in the State in accordance with the requirements of paragraph (2).

(ii) **EXCEPTION.**—Clause (i) shall not apply to any election contest for which the State or jurisdiction conducts a full recount through a manual adjudication of voter intent.

(B) **FULL MANUAL TABULATION.**—If a risk-limiting audit conducted under subparagraph (A) corrects the reported outcome of an election contest, the State or jurisdiction shall use the results of the manual adjudication of voter intent conducted as part of the risk-limiting audit as the official results of the election contest.

(2) **AUDIT REQUIREMENTS.**—

(A) **RULES AND PROCEDURES.**—

(i) **IN GENERAL.**—Not later than 1 year after the date of the enactment of this section, the chief State election official of the State shall establish rules and procedures for conducting risk-limiting audits.

(ii) **MATTERS INCLUDED.**—The rules and procedures established under clause (i) shall include the following:

(I) Rules and procedures for ensuring the security of ballots and documenting that prescribed procedures were followed.

(II) Rules and procedures for ensuring the accuracy of ballot manifests produced by jurisdictions.

(III) Rules and procedures for governing the format of ballot manifests and other data involved in risk-limiting audits.

(IV) Methods to ensure that any cast vote records used in a risk-limiting audit are those used by the voting system to tally the results of the election contest sent to the chief State election official of the State and made public.

(V) *Rules and procedures for the random selection of ballots to be inspected manually during each audit.*

(VI) *Rules and procedures for the calculations and other methods to be used in the audit and to determine whether and when the audit of each election contest is complete.*

(VII) *Rules and procedures for testing any software used to conduct risk-limiting audits.*

**(B) PUBLIC REPORT.—**

(i) *IN GENERAL.—After the completion of the risk-limiting audit and at least 5 days before the election contest is certified, the State shall publish a report on the results of the audit, together with such information as necessary to confirm that the audit was conducted properly.*

(ii) *FORMAT OF DATA.—All data published with the report under clause (i) shall be published in machine-readable, open data formats.*

(iii) *PROTECTION OF ANONYMITY OF VOTES.—Information and data published by the State under this subparagraph shall not compromise the anonymity of votes.*

(c) *EFFECTIVE DATE.—Each State and jurisdiction shall be required to comply with the requirements of this section for the first regularly scheduled election for Federal office held more than 1 year after the date of the enactment of the Securing America’s Federal Elections Act and for each subsequent election for Federal office.*

\* \* \* \* \*

**TITLE IV—ENFORCEMENT**

**SEC. 401. ACTIONS BY THE ATTORNEY GENERAL FOR DECLARATORY AND INJUNCTIVE RELIEF.**

The Attorney General may bring a civil action against any State or jurisdiction in an appropriate United States District Court for such declaratory and injunctive relief (including a temporary restraining order, a permanent or temporary injunction, or other order) as may be necessary to carry out the uniform and non-discriminatory election technology and administration requirements under sections 301, 302, [and 303] 303, and 303A.

\* \* \* \* \*

**TITLE IX—MISCELLANEOUS PROVISIONS**

**[SEC. 901. STATE DEFINED.**

**[In this Act, the term “State” includes the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, and the United States Virgin Islands.]**

**SEC. 901. DEFINITIONS.**

*In this Act, the following definitions apply:*

(1) *The term “cybersecurity incident” has the meaning given the term “incident” in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148).*

(2) *The term “election agency” means any component of a State, or any component of a unit of local government in a State, which is responsible for the administration of elections for Federal office in the State.*

(3) *The term “election infrastructure” means storage facilities, polling places, and centralized vote tabulation locations used to support the administration of elections for public office, as well as related information and communications technology, including voter registration databases, voting machines, 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 other systems used to manage the election process and to report and display election results on behalf of an election agency.*

(4) *The term “State” means each of the several States, the District of Columbia, the Commonwealth of Puerto Rico, Guam, American Samoa, the United States Virgin Islands, and the Commonwealth of the Northern Mariana Islands.*

\* \* \* \* \*

## SUPPLEMENTAL VIEW

The Republicans of the Committee on House Administration believe the integrity of our nation's elections and election infrastructure is of the utmost importance. This should not be a partisan issue. Unfortunately, the Majority, under pressure from its leadership, stepped away from bipartisan discussions for a joint election security bill. They rushed this partisan election security bill to a House Administration Committee markup in just over 48-hours, despite not having been considered in a Committee hearing, while a premature notice for a House Rules Committee hearing was released before the bill was voted out of Committee.

Democrats seem to believe burdensome and ineffective federal mandates, combined with an egregious amount of taxpayer funds, will solve the problems within election security. Unfortunately, this bill does very little to further secure our election systems and its proposed policies only hurt the state and local election officials it claims to help. Federally mandating the use of paper ballots and manual hand counts is a step backward for this country and erases all the hard work of state and local election officials across this country. Additionally, the Democrats are blindly committing \$1.3 billion over the course of 10 years. The Majority fails to remember that the funding of elections is the primary responsibility of the states.

Republicans introduced six amendments in the committee markup, including the requirement of a 25% funding match from states, which would force states receiving funds to have their own skin-in-the-game; prohibiting the practice of ballot harvestings; and introduced H.R. 3412, the Election Security Assistance Act, which provides states the resources they need to secure their elections, instead of burdensome and ineffective federal mandates. Democrats rejected all six of the Republicans' amendments.

RODNEY DAVIS.

○