AMENDMENT NO. _________  Calendar No. _________

Purpose: In the nature of a substitute.


S. 2593

To protect the administration of Federal elections against cybersecurity threats.

Referred to the Committee on ______________________ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Mr. BLUNT (for himself and Ms. KLOBUCHAR)

Viz:

1 Strike all after the enacting clause and insert the fol-
2 lowing:

3 SECTION 1. SHORT TITLE.

4 This Act may be cited as the “Secure Elections Act”.

5 SEC. 2. DEFINITIONS.

6 In this Act:

7 (1) APPROPRIATE CONGRESSIONAL COMMIT-
8 TEES.—The term “appropriate congressional com-
9 mittees” means—

10 (A) the Committee on Rules and Adminis-
11 tration, the Committee on Armed Services, the
Committee on Homeland Security and Governmental Affairs, the Committee on Appropriations, the Select Committee on Intelligence, the majority leader, and the minority leader of the Senate; and

(B) the Committee on House Administration, the Committee on Armed Services, the Committee on Homeland Security, the Committee on Appropriations, the Permanent Select Committee on Intelligence, the Speaker, and the minority leader of the House of Representatives.

(2) APPROPRIATE FEDERAL ENTITIES.—The term “appropriate Federal entities” means—

(A) the Department of Commerce, including the National Institute of Standards and Technology;

(B) the Department of Defense;

(C) the Department, including the component of the Department that reports to the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department;

(D) the Department of Justice, including the Federal Bureau of Investigation;
(E) the Commission; and

(F) the Office of the Director of National Intelligence, the National Security Agency, and such other elements of the intelligence community (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 3003)) as the Director of National Intelligence determines are appropriate.

(3) COMMISION.—The term “Commission” means the Election Assistance Commission.


(5) DEPARTMENT.—The term “Department” means the Department of Homeland Security.

(6) ELECTION AGENCY.—The term “election agency” means any component of a State or any component of a county, municipality, or other subdivision of a State that is responsible for administering Federal elections.

(7) ELECTION CYBERSECURITY INCIDENT.—The term “election cybersecurity incident” means any cybersecurity incident involving an election system.
(8) Election cybersecurity threat.—The term “election cybersecurity threat” means any cybersecurity threat (as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501)) to an election system.

(9) Election cybersecurity vulnerability.—The term “election cybersecurity vulnerability” means any security vulnerability (as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501)) that affects an election system.

(10) Election service provider.—The term “election service provider” means any person providing, supporting, or maintaining an election system on behalf of an election agency, such as a contractor or vendor.

(11) Election system.—The term “election system” means a voting system, an election management system, a voter registration website or database, an electronic pollbook, a system for tabulating or reporting election results, an election agency communications system, or any other information system (as defined in section 3502 of title 44, United States Code) that the Secretary, in consultation with the Commission, identifies as central to the manage-
ment, support, or administration of a Federal elec-

tion.

(12) **Federal election.**—The term “Federal
election” means a general, special, primary, or run-
off election for the office of President or Vice Presi-
dent, or of a Senator or Representative in, or Dele-
gate or Resident Commissioner to, the Congress that
is conducted by an election agency.

(13) **Federal entity.**—The term “Federal
entity” means any agency (as defined in section 551
of title 5, United States Code).

(14) **Secretary.**—The term “Secretary”
means the Secretary of Homeland Security.

(15) **Significant cybersecurity incident.**—The term “significant cybersecurity inci-
dent” is a cybersecurity incident that is, or a group
of related cybersecurity incidents that together are,
likely to result in demonstrable harm to the national
security interests, foreign relations, or economy of
the United States or to the public confidence, civil
liberties, or public health and safety of the American
people.

(16) **Significant election cybersecurity
incident.**—The term “significant election cyberse-
“security incident” means any significant cybersecurity incident involving an election system.

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

(18) STATE ELECTION OFFICIAL.—The term “State election official” means—

(A) the chief State election official of a State designated under section 10 of the National Voter Registration Act of 1993 (52 U.S.C. 20509); or

(B) in the Commonwealth of Puerto Rico, Guam, American Samoa, the Commonwealth of Northern Mariana Islands, and the United States Virgin Islands, a chief State election official designated by the State for purposes of this Act.

(19) STATE LAW ENFORCEMENT OFFICER.—The term “State law enforcement officer” means the head of a State law enforcement agency, such as an attorney general.
(20) Voting system.—The term “voting system” has the meaning given the term in section 301(b) of the Help America Vote Act of 2002 (52 U.S.C. 21081(b)).

SEC. 3. INFORMATION SHARING.

(a) Designation of Responsible Federal Entity.—The Secretary shall have primary responsibility within the Federal Government for sharing information about election cybersecurity incidents, threats, and vulnerabilities with Federal entities and with election agencies.

(b) Presumption of Federal Information Sharing to the Department.—If a Federal entity receives information about an election cybersecurity incident, threat, or vulnerability, the Federal entity shall promptly share that information with the Department, unless the head of the entity (or a Senate-confirmed official designated by the head) makes a specific determination in writing that there is good cause to withhold the particular information.

(c) Establishment of Information Sharing Plans and Protocols.—

(1) In general.—The Secretary shall establish and maintain a communication plan and protocols to
promptly share information related to election cybersecurity incidents, threats, and vulnerabilities.

(2) CONTENTS.—The communication plan and protocols required to be established under paragraph (1) shall require that the Department promptly share appropriate information with—

(A) the appropriate Federal entities;

(B) all State election officials;

(C) to the maximum extent practicable, all election agencies that have requested ongoing updates on election cybersecurity incidents, threats, or vulnerabilities; and

(D) to the maximum extent practicable, all election agencies that may be affected by the risks associated with the particular election cybersecurity incident, threat, or vulnerability.

(d) DEVELOPMENT OF STATE ELECTION CYBERSECURITY INCIDENT RESPONSE AND COMMUNICATION PLAN TEMPLATE.—The Secretary shall, in coordination with the Commission and the Election Infrastructure Government Coordinating Council, establish a template that a State may use when establishing a State election cybersecurity incident response and communication plan.

(e) TECHNICAL RESOURCES FOR ELECTION AGENCIES.—In sharing information about election cyberse-
rity incidents, threats, and vulnerabilities with election agencies under this section, the Department shall, to the maximum extent practicable—

(1) provide cyber threat indicators and defensive measures (as such terms are defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501)), such as recommended technical instructions, that assist with preventing, mitigating, and detecting threats or vulnerabilities;

(2) identify resources available for protecting against, detecting, responding to, and recovering from associated risks, including technical capabilities of the Department; and

(3) provide guidance about further sharing of the information.

(f) DECLASSIFICATION REVIEW.—If the Department receives classified information about an election cybersecurity incident, threat, or vulnerability—

(1) the Secretary shall promptly submit a request for expedited declassification review to the head of a Federal entity with authority to conduct the review, consistent with Executive Order 13526 or any successor order, unless the Secretary determines that such a request would be harmful to national security; and
(2) the head of the Federal entity described in paragraph (1) shall promptly conduct the review.

(g) Role of Non-Federal Entities.—The Department may share information about election cybersecurity incidents, threats, and vulnerabilities through a non-Federal entity.

(h) Protection of Personal and Confidential Information.—

(1) In General.—If a Federal entity shares or receives information relating to an election cybersecurity incident, threat, or vulnerability, the Federal entity shall, within Federal information systems (as defined in section 3502 of title 44, United States Code) of the entity—

(A) minimize the acquisition, use, and disclosure of personal information of voters, except as necessary to identify, protect against, detect, respond to, or recover from election cybersecurity incidents, threats, and vulnerabilities;

(B) notwithstanding any other provision of law, prohibit the retention of personal information of voters, such as—

(i) voter registration information, including physical address, email address, and telephone number;
(ii) political party affiliation or registration information; and

(iii) voter history, including registration status or election participation; and

(C) protect confidential Federal and State information from unauthorized disclosure.

(2) EXEMPTION FROM DISCLOSURE.—Information relating to an election cybersecurity incident, threat, or vulnerability, such as personally identifiable information of reporting persons or individuals affected by such incident, threat, or vulnerability, shared by or with the Federal Government shall be—

(A) deemed voluntarily shared information and exempt from disclosure under section 552 of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records; and

(B) withheld, without discretion, from the public under section 552(b)(3)(B) of title 5, United States Code, and any State, tribal, or local provision of law requiring disclosure of information or records.

(i) DUTY TO ASSESS POSSIBLE CYBERSECURITY INCIDENTS.—
(1) Election Agencies.—If an election agency becomes aware of the possibility of an election cybersecurity incident, the election agency shall promptly—

(A) assess whether an election cybersecurity incident occurred;

(B) notify the State election official in accordance with any notification process established by the State election official; and

(C) notify the Department in accordance with subsection (j).

(2) Election Service Providers.—If an election service provider becomes aware of the possibility of an election cybersecurity incident, the election service provider shall promptly—

(A) assess whether an election cybersecurity incident occurred; and

(B) notify the relevant election agencies in accordance with subsection (k).

(j) Information Sharing About Cybersecurity Incidents by Election Agencies.—If an election agency has reason to believe that an election cybersecurity incident has occurred with respect to an election system owned, operated, or maintained by or on behalf of the election agency, the election agency shall, in the most expe-
dient time possible and without unreasonable delay, pro-
vide notification of the election cybersecurity incident to
the Department in accordance with any notification proc-
ess established by the Secretary.

(k) INFORMATION SHARING ABOUT CYBERSECURITY
INCIDENTS BY ELECTION SERVICE PROVIDERS.—If an
election service provider has reason to believe that an elec-
tion cybersecurity incident may have occurred, or that an
incident related to the role of the provider as an election
service provider may have occurred, the election service
provider shall—

(1) notify the relevant election agencies in the
most expedient time possible and without unreason-
able delay; and

(2) cooperate with the election agencies in pro-
viding the notifications required under subsections
(i)(1) and (j).

(l) CONTENT OF NOTIFICATION BY ELECTION AGEN-
cies.—The notifications required under subsections (i)(1)
and (j)—

(1) shall include an initial assessment of—

(A) the date, time, and time zone when the
election cybersecurity incident began, if known;

(B) the date, time, and time zone when the
election cybersecurity incident was detected;
(C) the date, time, and duration of the election cybersecurity incident;

(D) the circumstances of the election cybersecurity incident, including the specific election systems believed to have been accessed and information acquired; and

(E) planned and implemented technical measures to respond to and recover from the incident; and

(2) shall be updated with additional material information, including technical data, as it becomes available.

(m) SECURITY CLEARANCE.—Not later than 30 days after the date of enactment of this Act, the Secretary—

(1) shall establish an expedited process for providing appropriate security clearance to State election officials and designated technical personnel employed by State election agencies;

(2) shall establish an expedited process for providing appropriate security clearance to members of the Commission and designated technical personnel employed by the Commission; and

(3) shall establish a process for providing appropriate security clearance to personnel at other election agencies.
(n) Protection From Liability.—Nothing in this Act may be construed to provide a cause of action against a State, unit of local government, or an election service provider.

(o) Assessment of Inter-state Information Sharing About Election Cybersecurity.—

(1) In General.—The Secretary and the Commission, in coordination with the heads of the appropriate Federal entities and appropriate officials of State and local governments, shall conduct an assessment of—

(A) the structure and functioning of the Elections Infrastructure Information Sharing and Analysis Center for purposes of election cybersecurity; and

(B) other mechanisms for inter-state information sharing about election cybersecurity.

(2) Comment From Election Agencies.—In carrying out the assessment required under paragraph (1), the Secretary and the Commission shall solicit and consider comments from all State election agencies.

(3) Distribution.—The Secretary and the Commission shall jointly issue the assessment required under paragraph (1) to—
(A) all election agencies known to the Department and the Commission; and

(B) the appropriate congressional committees.

(p) CONGRESSIONAL NOTIFICATION.—If an appropriate Federal entity has reason to believe that a significant election cybersecurity incident has occurred, the entity shall—

(1) not later than 7 calendar days after the date on which there is a reasonable basis to conclude that the significant election cybersecurity incident has occurred, provide notification of the significant election cybersecurity incident to the appropriate congressional committees; and

(2) update the initial notification under paragraph (1) within a reasonable period of time after additional information relating to the significant election cybersecurity incident is discovered.

SEC. 4. REQUIREMENT FOR THE ESTABLISHMENT OF CYBERSECURITY INCIDENT RESPONSE PLANS.

(a) IN GENERAL.—Subtitle D of title II of the Help America Vote Act of 2002 (52 U.S.C. 20901 et seq.) is amended by adding at the end the following new part:
“PART 7—REQUIREMENTS FOR ELECTION ASSISTANCE

“SEC. 297. ELECTION CYBERSECURITY INCIDENT RESPONSE AND COMMUNICATION PLANS.

“No State may receive any grant awarded under this Act after the date of the enactment of this section unless such State has established a response and communication plan with respect to election cybersecurity incidents (as defined in section 2(7) of the Secure Elections Act).”.

(b) CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Help America Vote Act of 2002 is amended by inserting after the item relating to section 296 the following:

“PART 7—REQUIREMENTS FOR ELECTION ASSISTANCE

“Sec. 297. Election cybersecurity incident response and communication plans.”.

SEC. 5. ELECTION CYBERSECURITY AND ELECTION AUDIT GUIDELINES.

(a) DEVELOPMENT BY TECHNICAL ADVISORY BOARD.—

(1) IN GENERAL.—

(A) ADDITIONAL DUTIES.—Section 221(b)(1) of the Help America Vote Act of 2002 (52 U.S.C. 20961(b)(2)) is amended by striking “in the development of the voluntary voting system guidelines” and inserting “in the development of—
“(A) the voluntary voting system guidelines;

“(B) the voluntary election cybersecurity guidelines (referred to in this part as the ‘election cybersecurity guidelines’) in accordance with paragraph (3); and

“(C) the voluntary election audit guidelines (referred to in this part as the ‘election audit guidelines’) in accordance with paragraph (4).”.

(B) CONFORMING AMENDMENTS.—Sections 202(1) and 207(3) of the Help America Vote Act of 2002 (52 U.S.C. 20922(1) and 20927(3)) are each amended by striking “voluntary voting system”.

(2) MEMBERSHIP AND RENAMING OF TECHNICAL GUIDELINES DEVELOPMENT COMMITTEE.—

(A) MEMBERSHIP.—Section 221(c)(1) of the Help America Vote Act of 2002 (52 U.S.C. 20961(c)(1)) is amended—

(i) by striking “14” and inserting “19”; and

(ii) by striking subparagraphs (A) through (E) and inserting the following:

“(A) 2 Members of the Standards Board.

“(B) 2 Members of the Board of Advisors.

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

“(E) 2 representatives of the National Association of Secretaries of State 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.

“(F) 2 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.

“(G) A representative of the Department of Homeland Security who possesses technical and scientific expertise relating to cybersecurity and the administration of elections.

“(H) A representative of the Election Infrastructure Information Sharing and Analysis Center who possesses technical and scientific expertise relating to cybersecurity.
“(I) A representative of the National Association of State Chief Information Officers.

“(J) A representative of State election information technology directors selected by the National Association of State Election Directors.

“(K) A representative of a manufacturer of voting system hardware and software who possesses technical and scientific expertise relating to cybersecurity and the administration of elections.

“(L) A representative of a laboratory accredited under section 231(b) who possesses technical and scientific expertise relating to cybersecurity and the administration of elections.

“(M) A representative that is an academic or scientific researcher who possesses technical and scientific expertise relating to cybersecurity.

“(N) A representative who possesses technical and scientific expertise relating to the accessibility and usability of voting systems.”.

(B) RENAMING OF COMMITTEE.—

(i) IN GENERAL.—Section 221(a) of the Help America Vote Act of 2002 (52
U.S.C. 20961(a)) is amended by striking “Technical Guidelines Development Committee (hereafter in this part referred to as the ‘Development Committee’)” and inserting “Technical Advisory Board”.

(ii) CONFORMING AMENDMENTS.—

(I) Section 201 of such Act (52 U.S.C. 20921) is amended by striking “Technical Guidelines Development Committee” and inserting “Technical Advisory Board”.

(II) Section 221 of such Act (52 U.S.C. 20921) is amended by striking “Development Committee” each place it appears and inserting “Technical Advisory Board”.

(III) Section 222(b) of such Act (52 U.S.C. 20962(b)) is amended—

(aa) by striking “Technical Guidelines Development Committee” in paragraph (1) and inserting “Technical Advisory Board”,

(bb) by striking “DEVELOPMENT COMMITTEE” in the head-
ing and inserting “TECHNICAL
ADVISORY BOARD”, and

(IV) Section 271(e) of such Act
(52 U.S.C. 21041(e)) is amended by
striking “Technical Guidelines Devel-
opment Committee” and inserting
“Technical Advisory Board”.

(V) Section 281(d) of such Act
(52 U.S.C. 21051(d)) is amended by
striking “Technical Guidelines Devel-
opment Committee” and inserting
“Technical Advisory Board”.

(VI) The heading for section
221 of such Act (52 U.S.C. 20961) is
amended by striking “TECHNICAL
GUIDELINES DEVELOPMENT COM-
MITTEE” and inserting “TECHNICAL
ADVISORY BOARD”.

(VII) The heading for part 3 of
subtitle A of title II of such Act is
amended by striking “TECHNICAL
GUIDELINES DEVELOPMENT COM-
MITTEE” and inserting “TECHNICAL
ADVISORY BOARD”.


(VIII) The items relating to section 221 and part 3 of title II in the table of contents of such Act are each amended by striking “Technical Guidelines Development Committee” and inserting “Technical Advisory Board”.

(b) GUIDELINES.—

(1) ELECTION CYBERSECURITY GUIDELINES.—

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.—

“(A) IN GENERAL.—The election cybersecurity guidelines shall contain guidelines for election cybersecurity, including standards for procuring, maintaining, testing, operating, and updating election systems.

“(B) REQUIREMENTS.—In developing the guidelines, the Technical Advisory Board shall—

“(i) identify the top risks to election systems;
“(ii) describe how specific technology choices can increase or decrease those risks; and

“(iii) provide recommended policies, best practices, and overall security strategies for identifying, protecting against, detecting, responding to, and recovering from the risks identified under subparagraph (A).

“(C) ISSUES CONSIDERED.—

“(i) IN GENERAL.—In developing the election cybersecurity guidelines, the Technical Advisory Board shall consider—

“(I) applying established cybersecurity best practices to Federal election administration by States and local governments, including appropriate technologies, procedures, and personnel for identifying, protecting against, detecting, responding to, and recovering from election cybersecurity incidents, threats, and vulnerabilities;

“(II) providing actionable guidance to election agencies that seek to
implement additional cybersecurity protections; and

“(III) any other factors that the Technical Advisory Board determines to be relevant.

“(D) Relationship to Voluntary Voting System Guidelines and National Institute of Standards and Technology Cybersecurity Guidance.—In developing the election cybersecurity guidelines, the Technical Advisory Board shall consider—

“(i) the voluntary voting system guidelines; and

“(ii) cybersecurity standards and best practices developed by the National Institute of Standards and Technology, including frameworks, consistent with section 2(c) of the National Institute of Standards and Technology Act (15 U.S.C. 272(c)).”.

(2) Audit Guidelines.—Section 221(b) of such Act (52 U.S.C. 20961(b)), as amended by paragraph (1), is amended by adding at the end the following new paragraph:

“(4) Election Audit Guidelines.—
“(A) IN GENERAL.—The election audit guidelines shall include provisions regarding voting systems and statistical audits for Federal elections, including that—

“(i) each vote is cast using a voting system that allows the voter an opportunity to inspect and confirm the marked ballot before casting it (consistent with accessibility requirements); and

“(ii) each election result is determined by tabulating marked ballots, and prior to the date on which the winning Federal candidate in the election is sworn into office, election agencies within the State inspect a random sample of the marked ballots and thereby establish high statistical confidence in the election result.

“(B) ISSUES CONSIDERED.—In developing the election audit guidelines, the Technical Advisory Board shall consider—

“(i) specific types of election audits, including procedures and shortcomings for such audits;

“(ii) mechanisms to verify that election systems accurately tabulate ballots, re-
port results, and identify a winner for each
election for Federal office, even if there is
an error or fault in the voting system;

“(iii) durational requirements needed
to facilitate election audits in a timely
manner that allows for confidence in the
outcome of the election prior to the swear-
ing-in of a Federal candidate, including
variations in the acceptance of postal bal-
 lots, time allowed to cure provisional bal-
 lots, and election certification deadlines;
and

“(iv) any other factors that the Tech-
nical Advisory Board considers to be rel-
evant.”.

(3) DEADLINES.—Section 221(b)(2) of such
Act (52 U.S.C. 20961(b)(2)), as amended by this
Act, is amended—

(A) by striking “The Technical” and in-
serting the following:

“(A) VOLUNTARY VOTING SYSTEM GUIDE-
LINES.—The Technical”;

(B) by striking “this section” and insert-
ing “paragraph (1)(A)”; and
(C) by adding at the end the following new subparagraph:

“(B) Election cybersecurity and election audit guidelines.—

“(i) Initial guidelines.—The Technical Advisory Board shall provide its initial set of recommendations under subparagraphs (B) and (C) of paragraph (1) to the Executive Director not later than 180 days after the date of the enactment of the Secure Elections Act.

“(ii) Periodic review.—Not later than March 31, 2021, and once every 2 years thereafter, the Technical Advisory Board shall review and update the guidelines described in subparagraphs (B) and (C) of paragraph (1).”.

(c) Process for Adoption.—

(1) Publication of recommendations.—

Section 221(f) of the Help America Vote Act of 2002 (52 U.S.C. 20961(f)) is amended—

(A) by striking “At the time the Commission” and inserting the following:

“(1) Voluntary voting system guidelines.—At the time the Commission”; and.
(B) by adding at the end the following new paragraph:

“(2) ELECTION CYBERSECURITY AND ELECTION AUDIT GUIDELINES.—The Technical Advisory Board shall—

“(A) provide a reasonable opportunity for public comment, including through Commission publication in the Federal Register, on the guidelines required under subparagraphs (B) and (C) of subsection (b)(1), including a 45-day opportunity for public comment on a draft of the guidelines before they are submitted to Congress under section 223(a), which shall, to the extent practicable, occur concurrently with the other activities of the Technical Advisory Board under this section with respect to such guidelines; and

“(B) consider the public comments in developing the guidelines.”.

(2) ADOPTION.—

(A) IN GENERAL.—Part 3 of subtitle A of title II of the Help America Vote Act of 2002 (52 U.S.C. 20961 et seq.) is amended—
(i) by inserting “OF VOLUNTARY VOTING GUIDELINES” after “ADOPTION” in the heading of section 222; and

(ii) by adding at the end the following new section:

“SEC. 223. PROCESS FOR ADOPTION OF ELECTION CYBER-SECURITY AND ELECTION AUDIT GUIDELINES.

“(a) Submission to Congress.—

“(1) In general.—Not later than 30 calendar days after the date on which the Commission receives recommendations for the guidelines described in subparagraphs (B) or (C) of section 221(b)(1), the Commission shall consider the guidelines and submit the guidelines to the appropriate congressional committees.

“(2) Modification.—In considering the guidelines, the Commission may modify the guidelines if—

“(A) the Commission determines that there is good cause to modify the guidelines, consistent with the considerations established in paragraphs (3) or (4) of section 221(b) (as the case may be) and notwithstanding the rec-
ommendation of the Technical Advisory Board;
and

“(B) the Commission submits a written
justification of the modification to the Tech-
nical Advisory Board and the appropriate con-
gressional committees.

“(b) DISTRIBUTION TO ELECTION AGENCIES.—The
Commission shall distribute the guidelines described in
subparagraphs (B) and (C) of section 221(b)(1) to all elec-
tion agencies known to the Commission.

“(c) PUBLICATION.—The Commission shall make the
guidelines described in subparagraphs (B) and (C) of sec-
tion 221(b)(1) available on the public website of the Com-
mision.

“(d) APPROPRIATE CONGRESSIONAL COMMITTEES.—
For purposes of this section, the term ‘appropriate con-
gressional committees’ means—

“(1) the Committee on Rules and Administra-
tion, the Committee on Armed Services, the Com-
mittee on Homeland Security and Governmental Af-
fairs, the Committee on Appropriations, the Select
Committee on Intelligence, the majority leader, and
the minority leader of the Senate; and

“(2) the Committee on House Administration,
the Committee on Armed Services, the Committee
on Homeland Security, the Committee on Appropriations, the Permanent Select Committee on Intelligence, the Speaker, and the minority leader of the House of Representatives.

“(e) RULE OF CONSTRUCTION.—Nothing in this section shall be construed to subject the process for developing the guidelines described in subparagraphs (B) and (C) of section 221(b)(1) to subchapter II of chapter 5, and chapter 7, of title 5, United States Code (commonly known as the ‘Administrative Procedure Act’).”.

(B) CLERICAL AMENDMENT.—The table of contents of such Act is amended by inserting after the item relating to section 222 the following new item:

“Sec. 223. Process for adoption of election cybersecurity and election audit guidelines.”.

SEC. 6. REQUIREMENT TO CONDUCT POST-ELECTION AUDITS.

(a) REQUIREMENT.—

(1) IN GENERAL.—Subtitle A of title III of the Help America Vote Act of 2002 (52 U.S.C. 21081 et seq.) is amended—

(A) by redesignating sections 304 and 305 as sections 305 and 306, respectively; and

(B) by inserting after section 303 the following new section:
“SEC. 304. POST-ELECTION AUDITS.

“(a) IN GENERAL.—Each State and jurisdiction shall—

“(1) conduct a post-election audit of each Federal election (as defined in section 2 of the Secure Elections Act) through the inspection of a random sample of marked ballots of sufficient quantity to establish high statistical confidence in the election result, as determined by the chief State election official;

“(2) provide a description of the planned audit, excluding any information deemed to create a security risk, to be conducted under paragraph (1) on a public website administered by the chief State election official 90 days prior to each such Federal election; and

“(3) provide results of the completed audit under paragraph (1) on a public website administered by the chief State election official within 10 days of the completion of the audit.

“(b) TIME FOR COMPLETING AUDIT.—The audit required by subsection (a) shall be completed in a timely manner to ensure confidence in the outcome of the election and before the date on which the winning candidate in the election is sworn into office.

“(c) 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 for the regularly scheduled general election for Federal office held in November 2020, and each subsequent election for Federal office.

“(2) WAIVER.—If a State or jurisdiction certifies to the Commission not later than November 1, 2020, that the State or jurisdiction will not meet the deadline described in paragraph (1) for good cause and includes in the certification the reasons for the failure to meet such deadline, paragraph (1) shall apply to the State or jurisdiction as if the reference in such subparagraph to ‘November 2020’ were a reference to ‘November 2022’.”.

(2) CLERICAL AMENDMENT.—The table of contents of such Act is amended—

(A) by redesignating the items relating to sections 304 and 305 as relating to sections 305 and 306, respectively; and

(B) by inserting after the item relating to section 303 the following new item:

“Sec. 304. Post-election audits.”.

(b) REPORTING.—The Election Assistance Commission shall—
(1) collect information regarding audits conducted by States under section 304 of the Help America Vote Act of 2002 (as added by subsection (a)); and

(2) submit reports to Congress on the information provided by the States under section 304(a)(2) and 304(a)(3) of such Act (as so added) and other information collected by the Commission under paragraph (1).

The reports under paragraph (2) shall be submitted concurrently with the reports required under section 9(a)(3) of the National Voter Registration Act of 1993.

SEC. 7. REQUIREMENT FOR PAPER BALLOTS.

(a) IN GENERAL.—Part 7 of subtitle D of title II of the Help America Vote Act of 2002, as added by section 4, is amended by adding at the end the following new section:

“SEC. 298. PAPER BALLOTS.

“No State or jurisdiction may use any grant awarded under this Act after the date of the enactment of this section to obtain voting equipment unless such voting equipment exclusively records each vote on a marked, individualized, readable paper ballot and allows the voter an opportunity to inspect and confirm the marked ballot (con-
sistent with accessibility requirements under Federal law) before the ballot is cast and counted.”.

(b) CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Help America Vote Act of 2002, as amended by section 4, is amended by inserting after the item relating to section 297 the following:

“Sec. 298. Paper ballots.”.

SEC. 8. STREAMLINING THE COLLECTION OF ELECTION INFORMATION.

Section 202 of the Help America Vote Act of 2002 (52 U.S.C. 20922) is amended by adding at the end the following flush sentence:

“Subchapter I of chapter 35 of title 44, United States Code, shall not apply to the collection of information for purposes of maintaining any clearinghouse with respect to the administration of Federal elections or the experiences of State and local governments in implementing the guidelines described in paragraph (1) or in operating voting systems in general.”.

SEC. 9. REPORTS TO CONGRESS ON FOREIGN THREATS TO ELECTIONS.

(a) IN GENERAL.—Not later than 30 days after the date of enactment of this Act, and 30 days after the end of each fiscal year thereafter, the Secretary and the Director of National Intelligence, in coordination with the heads of the appropriate Federal entities, shall submit a joint
report to the appropriate congressional committees on foreign threats to elections in the United States, including physical and cybersecurity threats.

(b) VOLUNTARY PARTICIPATION BY STATES.—The Secretary shall solicit and consider comments from all State election agencies. Participation by an election agency in the report under this subsection shall be voluntary and at the discretion of the State.