

115TH CONGRESS
1ST SESSION

S. 2261

To protect the administration of Federal elections against cybersecurity threats.

IN THE SENATE OF THE UNITED STATES

DECEMBER 21, 2017

Mr. LANKFORD (for himself, Ms. KLOBUCHAR, Mr. GRAHAM, Ms. HARRIS, Ms. COLLINS, and Mr. HEINRICH) introduced the following bill; which was read twice and referred to the Committee on Rules and Administration

A BILL

To protect the administration of Federal elections against cybersecurity threats.

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

3 **SECTION 1. SHORT TITLE.**

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

5 **SEC. 2. SENSE OF CONGRESS.**

6 It is the sense of Congress that—

7 (1) under the Constitution of the United States,
8 the States conduct elections, and Congress recog-

1 nizes the importance of maintaining State leadership
 2 in election administration;

3 (2) free and fair elections are central to our de-
 4 mocracy;

5 (3) protecting our elections is a national secu-
 6 rity priority; and

7 (4) an attack on our election systems by a for-
 8 eign power is a hostile act and should be met with
 9 appropriate retaliatory actions, including immediate
 10 and severe sanctions.

11 **SEC. 3. DEFINITIONS.**

12 In this Act:

13 (1) **ADVISORY PANEL.**—The term “Advisory
 14 Panel” means the advisory panel of independent ex-
 15 perts on election cybersecurity established under sec-
 16 tion 5(a)(1).

17 (2) **APPROPRIATE CONGRESSIONAL COMMIT-**
 18 **TEES.**—The term “appropriate congressional com-
 19 mittees” means—

20 (A) the Committee on Rules and Adminis-
 21 tration, the Committee on Armed Services, the
 22 Committee on Homeland Security and Govern-
 23 mental Affairs, the Committee on Appropria-
 24 tions, 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.

(3) 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

1 such other elements of the intelligence commu-
2 nity (as defined in section 3 of the National Se-
3 curity Act of 1947 (50 U.S.C. 3003)) as the
4 Director of National Intelligence determines are
5 appropriate.

6 (4) CHAIRMAN.—The term “Chairman” means
7 the Chairman of the Election Assistance Commis-
8 sion.

9 (5) COMMISSION.—The term “Commission”
10 means the Election Assistance Commission.

11 (6) DEPARTMENT.—The term “Department”
12 means the Department of Homeland Security.

13 (7) ELECTION AGENCY.—The term “election
14 agency” means any component of a State or any
15 component of a county, municipality, or other sub-
16 division of a State that is responsible for admin-
17 istering Federal elections.

18 (8) ELECTION CYBERSECURITY INCIDENT.—
19 The term “election cybersecurity incident” means
20 any information security incident involving an elec-
21 tion system.

22 (9) ELECTION CYBERSECURITY THREAT.—The
23 term “election cybersecurity threat” means any cy-
24 bersecurity threat (as defined in section 102 of the

1 Cybersecurity Information Sharing Act of 2015 (6
2 U.S.C. 1501)) to an election system.

3 (10) ELECTION CYBERSECURITY VULNER-
4 ABILITY.—The term “election cybersecurity vulner-
5 ability” means any security vulnerability (as defined
6 in section 102 of the Cybersecurity Information
7 Sharing Act of 2015 (6 U.S.C. 1501)) that affects
8 an election system.

9 (11) ELECTION SERVICE PROVIDER.—The term
10 “election service provider” means any person pro-
11 viding, supporting, or maintaining an election sys-
12 tem on behalf of an election agency, such as a con-
13 tractor or vendor.

14 (12) ELECTION SYSTEM.—The term “election
15 system” means any information system (as defined
16 in section 3502 of title 44, United States Code) used
17 for the management, support, or administration of a
18 Federal election, such as a voting system, a voter
19 registration website or database, an electronic
20 pollbook, a system for tabulating or reporting elec-
21 tion results, or an election agency email system.

22 (13) FEDERAL ELECTION.—The term “Federal
23 election” means any election (as defined in section
24 301(1) of the Federal Election Campaign Act of
25 1971 (52 U.S.C. 30101(1)) for Federal office (as

1 defined in section 301(3) of the Federal Election
2 Campaign Act of 1971 (52 U.S.C. 30101(3)).

3 (14) FEDERAL ENTITY.—The term “Federal
4 entity” means any agency (as defined in section 551
5 of title 5, United States Code).

6 (15) INCIDENT.—The term “incident” has the
7 meaning given the term in section 3552 of title 44,
8 United States Code.

9 (16) INFORMATION SECURITY.—The term “in-
10 formation security” has the meaning given the term
11 in section 3552 of title 44, United States Code.

12 (17) SECRETARY.—The term “Secretary”
13 means the Secretary of Homeland Security, or, upon
14 designation by the Secretary of Homeland Security,
15 the Deputy Secretary of Homeland Security, the
16 Under Secretary responsible for overseeing critical
17 infrastructure protection, cybersecurity, and other
18 related programs of the Department, or a Senate-
19 confirmed official that reports to that Under Sec-
20 retary.

21 (18) STATE.—The term “State” means each of
22 the several States of the United States, the District
23 of Columbia, the Commonwealth of Puerto Rico,
24 Guam, American Samoa, the Commonwealth of

1 Northern Mariana Islands, and the United States
 2 Virgin Islands.

3 (19) STATE ELECTION OFFICIAL.—The term
 4 “State election official” means—

5 (A) the chief State election official of a
 6 State designated under section 10 of the Na-
 7 tional Voter Registration Act of 1993 (52
 8 U.S.C. 20509); or

9 (B) in the Commonwealth of Puerto Rico,
 10 Guam, American Samoa, the Commonwealth of
 11 Northern Mariana Islands, and the United
 12 States Virgin Islands, a chief State election of-
 13 ficial designated by the State for purposes of
 14 this Act.

15 (20) STATE LAW ENFORCEMENT OFFICER.—
 16 The term “State law enforcement officer” means the
 17 head of a State law enforcement agency, such as an
 18 attorney general.

19 (21) VOTING SYSTEM.—The term “voting sys-
 20 tem” has the meaning given the term in section
 21 301(b) of the Help America Vote Act of 2002 (52
 22 U.S.C. 21081(b)).

23 **SEC. 4. INFORMATION SHARING.**

24 (a) DESIGNATION OF RESPONSIBLE FEDERAL ENTI-
 25 TY.—The Secretary shall have primary responsibility with-

1 in the Federal Government for sharing information about
 2 election cybersecurity incidents, threats, and
 3 vulnerabilities with Federal entities and with election
 4 agencies.

5 (b) PRESUMPTION OF FEDERAL INFORMATION
 6 SHARING TO THE DEPARTMENT.—If a Federal entity re-
 7 ceives information about an election cybersecurity inci-
 8 dent, threat, or vulnerability, the Federal entity shall
 9 promptly share that information with the Department, un-
 10 less the head of the entity (or a Senate-confirmed official
 11 designated by the head) makes a specific determination
 12 in writing that there is good cause to withhold the par-
 13 ticular information.

14 (c) PRESUMPTION OF FEDERAL AND STATE INFOR-
 15 MATION SHARING FROM THE DEPARTMENT.—If the De-
 16 partment receives information about an election cyberse-
 17 curity incident, threat, or vulnerability, unless the Sec-
 18 retary makes a specific determination in writing that there
 19 is good cause to withhold the particular information, the
 20 Department shall promptly share that information with—

- 21 (1) the appropriate Federal entities;
- 22 (2) all State election agencies;
- 23 (3) all election agencies that have requested on-
 24 going updates on election cybersecurity incidents,
 25 threats, or vulnerabilities; and

1 (4) all election agencies that may be affected by
2 the risks associated with the particular election cy-
3 bersecurity incident, threat, or vulnerability.

4 (d) TECHNICAL RESOURCES FOR ELECTION AGEN-
5 CIES.—In sharing information about election cybersecu-
6 rity incidents, threats, and vulnerabilities with election
7 agencies under this section, the Department shall, to the
8 extent possible—

9 (1) provide cyber threat indicators and defen-
10 sive measures (as such terms are defined in section
11 102 of the Cybersecurity Information Sharing Act of
12 2015 (6 U.S.C. 1501)), such as recommended tech-
13 nical instructions, that assist with protecting against
14 and detecting associated risks;

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

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

21 (e) DECLASSIFICATION REVIEW.—If the Department
22 receives classified information about an election cybersecu-
23 rity incident, threat, or vulnerability—

24 (1) the Secretary shall promptly submit a re-
25 quest for expedited declassification review to the

1 head of a Federal entity with authority to conduct
2 the review, consistent with Executive Order 13526
3 or any successor order; and

4 (2) the head of the Federal entity described in
5 paragraph (1) shall promptly conduct the review.

6 (f) ROLE OF NON-FEDERAL ENTITIES.—The De-
7 partment may share information about election cybersecu-
8 rity incidents, threats, and vulnerabilities through a non-
9 Federal entity, such as the Multi-State Information Shar-
10 ing and Analysis Center.

11 (g) PROTECTION OF PERSONAL AND CONFIDENTIAL
12 INFORMATION.—If a Federal entity shares information
13 about an election cybersecurity incident, threat, or vulner-
14 ability, the Federal entity shall—

15 (1) minimize the acquisition, retention, use, and
16 disclosure of personal information of voters, except
17 as necessary to identify, protect against, detect, re-
18 spond to, or recover from election cybersecurity inci-
19 dents, threats, and vulnerabilities; and

20 (2) take reasonable steps to protect confidential
21 Federal and State information from unauthorized
22 disclosure.

23 (h) DUTY TO ASSESS POSSIBLE CYBERSECURITY IN-
24 CIDENTS.—

1 (1) ELECTION AGENCIES.—If an election agen-
 2 cy becomes aware of the possibility of an election cy-
 3 bersecurity incident, the election agency shall
 4 promptly assess whether an election cybersecurity in-
 5 cident occurred and notify the State election official.

6 (2) ELECTION SERVICE PROVIDERS.—If an
 7 election service provider becomes aware of the possi-
 8 bility of an election cybersecurity incident, the elec-
 9 tion service provider shall promptly assess whether
 10 an election cybersecurity incident occurred and no-
 11 tify the relevant election agencies consistent with
 12 subsection (j).

13 (i) INFORMATION SHARING ABOUT CYBERSECURITY
 14 INCIDENTS BY ELECTION AGENCIES.—If an election
 15 agency has reason to believe that an election cybersecurity
 16 incident has occurred with respect to an election system
 17 owned, operated, or maintained by or on behalf of the elec-
 18 tion agency, the election agency shall, in the most expe-
 19 dient time possible and without unreasonable delay (in no
 20 event longer than 3 calendar days after discovery of the
 21 incident), provide notification of the election cybersecurity
 22 incident to the Secretary.

23 (j) INFORMATION SHARING ABOUT CYBERSECURITY
 24 INCIDENTS BY ELECTION SERVICE PROVIDERS.—If an
 25 election service provider has reason to believe that an elec-

tion cybersecurity incident may have occurred, or that an
 information security incident related to the role of the pro-
 vider 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 (in no event longer than 3 calendar days
 after discovery of the possible incident); and

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

(k) CONTENT OF NOTIFICATION BY ELECTION
 AGENCIES.—The notifications required under subsections
 (h)(1) and (i)—

(1) shall include an initial assessment of—

(A) the date and duration of the election
 cybersecurity incident;

(B) the circumstances of the election cy-
 bersecurity incident, including the specific elec-
 tion systems believed to have been accessed and
 information acquired; and

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

1 (2) shall be updated with additional material in-
2 formation, including technical data, as it becomes
3 available.

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

6 (1) shall establish an expedited process for pro-
7 viding appropriate security clearance to State elec-
8 tion officials and designated technical personnel em-
9 ployed by State election agencies;

10 (2) shall establish an expedited process for pro-
11 viding appropriate security clearance to members of
12 the Commission and designated technical personnel
13 employed by the Commission; and

14 (3) shall establish a process for providing ap-
15 propriate security clearance to personnel at other
16 election agencies.

17 (m) CATALOG OF CYBERSECURITY SERVICES.—The
18 Secretary—

19 (1) shall make publicly available, including on
20 the public website of the Department, a catalog of
21 cybersecurity services that the appropriate Federal
22 agencies can provide to election agencies and a point
23 of contact for each service; and

1 (2) may create a classified annex to the catalog
 2 and make it available only to election agency per-
 3 sonnel with appropriate security clearance.

4 (n) PROTECTION FROM LIABILITY.—Nothing in this
 5 Act may be construed to provide a cause of action against
 6 a State, unit of local government, or an election service
 7 provider.

8 (o) ASSESSMENT OF INTER-STATE INFORMATION
 9 SHARING ABOUT ELECTION CYBERSECURITY.—

10 (1) IN GENERAL.—The Secretary and the
 11 Chairman, in coordination with the heads of the ap-
 12 propriate Federal entities and appropriate officials
 13 of State and local governments, shall conduct an as-
 14 sessment of—

15 (A) the structure and functioning of the
 16 Multi-State Information Sharing and Analysis
 17 Center for purposes of election cybersecurity;
 18 and

19 (B) other mechanisms for inter-state infor-
 20 mation sharing about election cybersecurity.

21 (2) COMMENT FROM ELECTION AGENCIES.—In
 22 carrying out the assessment required under para-
 23 graph (1), the Secretary and the Chairman shall so-
 24 licit and consider comments from all State election
 25 agencies.

1 (3) DISTRIBUTION.—The Secretary and the
2 Chairman shall jointly issue the assessment required
3 under paragraph (1) to—

4 (A) all election agencies known to the De-
5 partment and the Commission; and

6 (B) the appropriate congressional commit-
7 tees.

8 (p) CONGRESSIONAL NOTIFICATION.—

9 (1) IN GENERAL.—If an appropriate Federal
10 entity has reason to believe that a significant elec-
11 tion cybersecurity incident has occurred, the entity
12 shall—

13 (A) not later than 7 calendar days after
14 the date on which there is a reasonable basis to
15 conclude that the significant incident has oc-
16 curred, provide notification of the incident to—

17 (i) the appropriate congressional com-
18 mittees;

19 (ii) the members of the Senate rep-
20 resenting the States affected by the inci-
21 dent; and

22 (iii) the members of the House of
23 Representatives representing the congres-
24 sional districts affected by the incident;
25 and

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

5 (2) REPORTING THRESHOLD.—The Secretary
6 shall—

7 (A) promulgate a uniform definition of a
8 “significant election cybersecurity incident”;
9 and

10 (B) shall submit the definition promul-
11 gated under subparagraph (A) to the appro-
12 priate congressional committees.

13 **SEC. 5. ADVISORY PANEL AND GUIDELINES.**

14 (a) ADVISORY PANEL.—

15 (1) IN GENERAL.—The Secretary shall establish
16 an advisory panel of independent experts on election
17 cybersecurity.

18 (2) MEMBERSHIP.—The Advisory Panel shall
19 consist of not less than 9 members, of whom—

20 (A) 5 shall be appointed by the Secretary,
21 in consultation with the Chairman and the Di-
22 rector of the National Institute of Standards
23 and Technology, of whom 1 shall be designated
24 as the Chairperson of the Advisory Panel;

1 (B) 1 shall be appointed by the National
2 Association of Secretaries of State;

3 (C) 1 shall be appointed by the National
4 Association of State Election Directors;

5 (D) 1 shall be appointed by the National
6 Association of Counties; and

7 (E) 1 shall be appointed by the National
8 League of Cities.

9 (3) ELIGIBILITY.—Individuals appointed to the
10 Advisory Panel established under paragraph (1)—

11 (A) may not be officers or employees of the
12 United States;

13 (B) if appointed under paragraph (2)(A),
14 shall possess expertise in cybersecurity; and

15 (C) if appointed under any other subpara-
16 graph of paragraph (2), shall possess expertise
17 in cybersecurity, election law, or election admin-
18 istration.

19 (4) TERMS; VACANCIES.—Members of the Advi-
20 sory Panel shall serve for a term set by the Sec-
21 retary. Any vacancy in the Advisory Panel shall be
22 filled in the same manner as the original appoint-
23 ment.

24 (5) COMPENSATION.—Members of the Advisory
25 Panel shall serve on the Advisory Panel without

1 compensation, except that members of the Advisory
2 Panel may be allowed travel expenses, including per
3 diem in lieu of subsistence, at rates authorized for
4 employees of agencies under subchapter I of chapter
5 57 of title 5, United States Code, while away from
6 their homes or regular places of business in the per-
7 formance of services for the Advisory Panel.

8 (6) ADMINISTRATIVE STAFF.—Upon request of
9 the Advisory Panel, the Secretary shall provide to
10 the Advisory Panel, on a reimbursable basis, the ad-
11 ministrative support services necessary for the Advi-
12 sory Panel to carry out its responsibilities under this
13 Act.

14 (b) GUIDELINES.—

15 (1) IN GENERAL.—The Advisory Panel shall de-
16 velop a set of guidelines for election cybersecurity,
17 including standards for procuring, maintaining, test-
18 ing, auditing, operating, and updating election sys-
19 tems.

20 (2) REQUIREMENTS.—In developing the guide-
21 lines, the Advisory Panel shall—

22 (A) identify the top risks to election sys-
23 tems;

1 (B) describe how specific technology
2 choices can increase or decrease those risks;
3 and

4 (C) provide recommended policies, best
5 practices, and overall security strategies for
6 identifying, protecting against, detecting, re-
7 sponding to, and recovering from the risks iden-
8 tified under subparagraph (A).

9 (c) GRANT PROGRAM.—The Advisory Panel shall as-
10 sist the Department and the Commission in carrying out
11 the grant program required under section 7 by—

12 (1) submitting recommendations to the Depart-
13 ment about the grant program application process;

14 (2) submitting recommendations, including rec-
15 ommended criteria, to the Department for the grant
16 program review process;

17 (3) submitting recommendations, including rec-
18 ommended criteria, to the Department for use of re-
19 maining grant funds;

20 (4) submitting recommendations, including rec-
21 ommended criteria, to the Department for the in-
22 terim grant program for non-paper equipment re-
23 placement; and

24 (5) providing any other assistance that the De-
25 partment or the Commission requests.

1 (d) PAPER BALLOTS AND STATISTICAL AUDITS.—

2 The guidelines developed under subsection (b) shall in-
 3 clude provisions regarding paper ballots and statistical au-
 4 dits for Federal elections, including that—

5 (1) each vote is made by a paper ballot (marked
 6 by hand or device), and the voter has an opportunity
 7 to inspect and confirm the marked paper ballot be-
 8 fore casting it (consistent with accessibility accom-
 9 modations); and

10 (2) each election result is determined by tab-
 11 ulating marked paper ballots (by hand or device),
 12 and prior to certification by a State of the election
 13 result, election agencies within the State inspect (by
 14 hand and not by device) a random sample of the
 15 marked paper ballots and thereby establish high sta-
 16 tistical confidence in the election result.

17 (e) ISSUES CONSIDERED.—

18 (1) IN GENERAL.—In developing the guidelines
 19 required under subsection (b), the Advisory Panel
 20 shall consider—

21 (A) applying established cybersecurity best
 22 practices to Federal election administration by
 23 States and local governments, including appro-
 24 priate technologies, procedures, and personnel
 25 for identifying, protecting against, detecting, re-

1 sponding to, and recovering from cybersecurity
2 events;

3 (B) mechanisms to verify that election sys-
4 tems accurately tabulate ballots, report results,
5 and identify a winner for each election for Fed-
6 eral office, even if computer hardware or soft-
7 ware malfunctions due to error or an election
8 cybersecurity incident;

9 (C) specific types of election audits, includ-
10 ing procedures and shortcomings for such au-
11 dits;

12 (D) durational requirements needed to fa-
13 cilitate election audits prior to election certifi-
14 cation, including variations in the acceptance of
15 postal ballots, time allowed to cure provisional
16 ballots, and election certification deadlines;

17 (E) providing actionable guidance to elec-
18 tion agencies that have not applied for or re-
19 ceived grant funds under section 7, and to
20 agencies that seek to implement additional cy-
21 bersecurity protections;

22 (F) how the guidelines could assist other
23 components of State and local governments;
24 and

1 (G) any other factors that the Advisory
2 Panel determines to be relevant.

3 (2) RELATIONSHIP TO VOLUNTARY VOTING
4 GUIDELINES AND NATIONAL INSTITUTE OF STAND-
5 ARDS AND TECHNOLOGY CYBERSECURITY GUID-
6 ANCE.—In developing the guidelines required under
7 subsection (b), the Advisory Panel shall consider—

8 (A) the Voluntary Voting Guidelines devel-
9 oped by the Commission; and

10 (B) cybersecurity standards and best prac-
11 tices developed by the National Institute of
12 Standards and Technology, including frame-
13 works, consistent with section 2(c) of the Na-
14 tional Institute of Standards and Technology
15 Act (15 U.S.C. 272(c)).

16 (f) PUBLIC COMMENT.—The Advisory Panel shall—

17 (1) provide a reasonable opportunity for public
18 comment, including through Department publication
19 in the Federal Register, on the guidelines required
20 under subsection (b), including a 45-day opportunity
21 for public comment on a draft of the guidelines be-
22 fore they are submitted under subsection (i), which
23 shall, to the extent practicable, occur concurrently
24 with the other activities of the Advisory Panel under
25 this section; and

1 (2) consider the public comments in developing
2 the guidelines.

3 (g) CONSULTATION.—In developing the guidelines re-
4 quired under subsection (b), the Advisory Panel shall con-
5 sult with—

6 (1) the appropriate Federal entities;

7 (2) the Standards Board, Board of Advisors,
8 and Technical Guidelines Development Committee of
9 the Commission;

10 (3) the Federal Communications Commission;

11 (4) the Federal Trade Commission;

12 (5) the National Governors Association;

13 (6) the National Association of Secretaries of
14 State;

15 (7) the National Association of State Election
16 Directors;

17 (8) the National Association of Election Offi-
18 cials;

19 (9) the National Association of Counties;

20 (10) the National League of Cities;

21 (11) the International Association of Govern-
22 ment Officials;

23 (12) the Multi-State Information Sharing and
24 Analysis Center;

25 (13) the National Science Foundation; and

1 (14) any other interested entities that the Advi-
2 sory Panel determines are necessary to the develop-
3 ment of the guidelines.

4 (h) SUBMISSION TO SECRETARY.—Not later than
5 180 days after the date of enactment of this Act, the Advi-
6 sory Panel shall submit the guidelines required under sub-
7 section (b) to the Secretary.

8 (i) SUBMISSION TO CONGRESS; MODIFICATION.—Not
9 later than 14 calendar days after the date on which the
10 Secretary receives guidelines under subsection (h) or (l),
11 the Secretary shall submit the guidelines to the appro-
12 priate congressional committees. The Secretary may mod-
13 ify the guidelines in advance of submission to Congress
14 if—

15 (1) the Secretary determines that there is good
16 cause to modify the guidelines, consistent with the
17 considerations established in subsection (e) and not-
18 withstanding the recommendation of the Advisory
19 Panel; and

20 (2) the Secretary submits a written justification
21 of the modification to the Advisory Panel and the
22 appropriate congressional committees.

23 (j) DISTRIBUTION TO ELECTION AGENCIES.—The
24 Secretary shall distribute the guidelines required under

1 subsection (b) to all election agencies known to the De-
2 partment and the Commission.

3 (k) PUBLICATION.—The Secretary shall make the
4 guidelines required under subsection (b) available on the
5 public website of the Department.

6 (l) PERIODIC REVIEW.—Not later than January 31,
7 2019, and once every 2 years thereafter, the Advisory
8 Panel shall review and update the guidelines required
9 under subsection (b).

10 (m) RULE OF CONSTRUCTION.—Nothing in the sec-
11 tion shall be construed to subject the process for devel-
12 oping the guidelines required under subsection (b) to sub-
13 chapter II of chapter 5, and chapter 7, of title 5, United
14 States Code (commonly known as the “Administrative
15 Procedure Act”).

16 **SEC. 6. REPORTS TO CONGRESS.**

17 (a) REPORTS ON FOREIGN THREATS TO ELEC-
18 TIONS.—

19 (1) IN GENERAL.—Not later than 30 days after
20 the date of enactment of this Act, and 30 days after
21 the end of each fiscal year thereafter, the Secretary
22 and the Director of National Intelligence, in coordi-
23 nation with the heads of the appropriate Federal en-
24 tities, shall submit a joint report to the appropriate
25 congressional committees on foreign threats to elec-

1 tions in the United States, including physical and
2 cybersecurity threats.

3 (2) VOLUNTARY PARTICIPATION BY STATES.—

4 The Secretary shall solicit and consider comments
5 from all State election agencies. Participation by an
6 election agency in the report under this subsection
7 shall be voluntary and at the discretion of the State.

8 (b) REPORTS ON GRANT PROGRAM.—Not later than
9 2 years after the date of enactment of this Act, and every
10 4 years thereafter, the Comptroller General of the United
11 States shall submit a report to the appropriate congres-
12 sional committees on the Department grant program es-
13 tablished under section 7, including how grant funds have
14 been distributed and used to implement the guidelines re-
15 quired under section 5(b).

16 **SEC. 7. STATE ELECTION SYSTEM CYBERSECURITY AND**
17 **MODERNIZATION GRANTS.**

18 (a) AUTHORITY.—

19 (1) IN GENERAL.—The Secretary, acting
20 through the component of the Department that re-
21 ports to the Under Secretary responsible for over-
22 seeing critical infrastructure protection, cybersecu-
23 rity, and other related programs of the Department,
24 shall award grants to States in accordance with this
25 section.

1 (2) COORDINATION.—

2 (A) IN GENERAL.—The Secretary shall co-
3 ordinate with the Commission in carrying out
4 this section.

5 (B) JOINT PROGRAM.—If the Secretary de-
6 termines that jointly carrying out this section
7 with the Commission would increase State par-
8 ticipation and cybersecurity preparedness, the
9 Secretary shall—

10 (i) submit notice of the determination
11 to the Committee on Homeland Security
12 and Governmental Affairs of the Senate
13 and the Committee on Homeland Security
14 of the House of Representatives; and

15 (ii) enter into a Memorandum of Un-
16 derstanding with the Commission to carry
17 out the grant program.

18 (b) APPLICATION PROCESS.—

19 (1) IN GENERAL.—The Secretary shall—

20 (A) establish a process for States to apply
21 for election system cybersecurity and mod-
22 ernization grants;

23 (B) in establishing the application process,
24 consider the recommendations of the Advisory
25 Panel under section 5(c); and

1 (C) ensure that the application process re-
2 quires that a State seeking a grant provide a
3 detailed explanation of how election agencies
4 within the State will implement the guidelines
5 established under section 5(b).

6 (2) REVIEW.—The Secretary—

7 (A) shall fund a State application if the
8 Secretary determines that—

9 (i) the election agencies within the
10 State will likely implement the guidelines
11 established under section 5(b);

12 (ii) with respect to the guidelines re-
13 lated to statistical audits, consistent with
14 section 5(d), the State will complete a
15 statewide pilot program during a biennial
16 Federal general election not later than
17 2022; and

18 (iii) the State will match at least ten
19 percent of the total grant allocation for
20 election cybersecurity improvements; and

21 (B) in reviewing a State application, shall
22 consider the recommendations and criteria of
23 the Advisory Panel under section 5(c).

24 (3) STATE IMPLEMENTATION.—

1 (A) IN GENERAL.—A State receiving a
2 grant under this section may adopt any reason-
3 able implementation of the guidelines estab-
4 lished under section 5(b).

5 (B) INCONSISTENCY WITH STATE LAW.—If
6 implementation of the guidelines would be in-
7 consistent with State law, the State—

8 (i) shall identify in the application of
9 the State the legal issue and the guidelines
10 that the State cannot implement;

11 (ii) shall specify in the application of
12 the State the amount of grant funds that
13 the State would spend implementing those
14 guidelines if the law were not inconsistent;
15 and

16 (iii) shall not spend the amount of
17 grant funds specified under clause (ii) until
18 the legal issue is resolved.

19 (4) PROTECTION OF PERSONAL INFORMA-
20 TION.—The application process established under
21 this subsection shall not require a State to disclose
22 the personal information of any voter.

23 (c) USE OF FUNDS.—

24 (1) IN GENERAL.—Except as provided in para-
25 graph (2), a State receiving a grant under this sec-

1 tion shall use the funds received under the grant to
 2 implement the guidelines established under section
 3 5(b).

4 (2) REMAINING FUNDS.—A State may use
 5 funds from a grant under this section to improve,
 6 upgrade, or acquire hardware, software, or services
 7 related to election administration, consistent with
 8 the guidelines established under section 5(b), if—

9 (A) the State election official submits a
 10 written certification to the Secretary that the
 11 election agencies within the State have imple-
 12 mented the guidelines established under section
 13 5(b); and

14 (B) the Secretary, after consideration of
 15 the recommendations and criteria of the Advi-
 16 sory Panel under section 5(c), approves the use
 17 of funds.

18 (3) PROHIBITION ON USE FOR CERTAIN VOTING
 19 SYSTEMS.—Funds received under a grant under this
 20 section may not be used for any voting system that
 21 records each vote in electronic storage unless the
 22 system is an optical scanner that reads paper bal-
 23 lots.

24 (d) CONTRACTING ASSISTANCE.—Not later than 90
 25 days after the date of enactment of this Act, the Adminis-

1 trator of General Services, in consultation with the Direc-
 2 tor of the National Institute of Standards and Technology,
 3 shall take such actions as may be necessary through com-
 4 petitive processes—

5 (1) to qualify a set of private sector entities
 6 that are capable of assisting the States with identi-
 7 fying, protecting against, detecting, responding to,
 8 and recovering from election cybersecurity incidents,
 9 threats, and vulnerabilities;

10 (2) to establish contract vehicles to enable
 11 States to access the services of 1 or more of the pri-
 12 vate sector organizations after receiving amounts
 13 under a grant under this section;

14 (3) to ensure that the contract vehicles permit
 15 individual States to augment Federal funds with
 16 funding otherwise available to the States; and

17 (4) to provide a list of qualified entities to the
 18 Secretary and Chairman in order to ensure it is
 19 readily available to State election officials.

20 (e) LIMITATION ON AMOUNT OF GRANT.—

21 (1) IN GENERAL.—Subject to paragraph (3),
 22 the amount of funds provided to a State under a
 23 grant under this section shall be equal to the prod-
 24 uct obtained by multiplying—

1 (A) the total amount appropriated for
2 grants pursuant to the authorization under sec-
3 tion 6; by

4 (B) the State allocation percentage for the
5 State (as determined under paragraph (2)).

6 (2) STATE ALLOCATION PERCENTAGE.—The
7 State allocation percentage for a State is the amount
8 (expressed as a percentage) equal to the quotient ob-
9 tained by dividing—

10 (A) the total voting age population of all
11 States (as reported in the most recent decennial
12 census); by

13 (B) the voting age population of the State
14 (as reported in the most recent decennial cen-
15 sus).

16 (3) MINIMUM AMOUNT OF PAYMENT.—The
17 amount determined under this subsection may not
18 be less than—

19 (A) in the case of any of the several States
20 or the District of Columbia, 0.5 percent of the
21 total amount appropriated for grants under this
22 section; or

23 (B) in the case of the Commonwealth of
24 Puerto Rico, Guam, American Samoa, the Com-
25 monwealth of Northern Mariana Islands, or the

1 United States Virgin Islands, 0.1 percent of
2 such total amount.

3 (4) PRO RATA REDUCTIONS.—The Secretary
4 shall make such pro rata reductions to the alloca-
5 tions determined under paragraph (1) as are nec-
6 essary to comply with the requirements of paragraph
7 (3).

8 (f) INTERIM GRANT PROGRAM FOR ELECTION PRE-
9 PAREDNESS.—

10 (1) IN GENERAL.—The Secretary shall award a
11 grant to an election agency, regardless of State sub-
12 mission of an application under subsection (b),
13 that—

14 (A) receives a “cyber hygiene” scan, a risk
15 and vulnerability assessment, or a similar cy-
16 bersecurity evaluation by the Department or a
17 contractor approved by the Department; and

18 (B) not later than November 6, 2018, sub-
19 mits to the Department—

20 (i) the results of the evaluation de-
21 scribed in subparagraph (A);

22 (ii) a plan for rapidly remediating the
23 vulnerabilities identified by the evaluation,
24 including specific expenditures; and

1 (iii) in the case of an application by
2 any election agency of a political subdivi-
3 sion of a State, a certification of approval
4 from the State election agency.

5 (2) PRIORITIZATION FOR LOCAL GOVERN-
6 MENTS.—A State election agency may authorize
7 some or all other election agencies within the State
8 to apply for interim grants under paragraph (1). If
9 the amount available under paragraph (5) is not suf-
10 ficient to fund the applications received from election
11 agencies within the State, the State election agency
12 may establish a priority order for funding applica-
13 tions.

14 (3) USE OF FUNDS.—An election agency that
15 receives a grant under paragraph (1) shall only use
16 the funds received under the grant to implement the
17 remediation plan submitted under paragraph
18 (1)(B)(ii).

19 (4) UNAVAILABILITY OF DEPARTMENT SERV-
20 ICES.—If an election agency requests an evaluation
21 by the Department consistent with paragraph
22 (1)(A), and the Department is not able to provide
23 the evaluation during the 30-calendar-day period fol-
24 lowing the request, the agency may—

1 (A) procure a reasonably equivalent eval-
 2 uation from a private-sector entity; and

3 (B) use funds received from a grant under
 4 subparagraph (A) as reimbursement for the
 5 cost of the evaluation.

6 (5) LIMITATION ON AMOUNT OF GRANT; CO-
 7 ORDINATION WITH CYBERSECURITY AND MOD-
 8 ERNIZATION GRANTS.—

9 (A) LIMITATION.—The aggregate amount
 10 of grants under this subsection to all election
 11 agencies in a State shall not exceed 10 percent
 12 of the limitation with respect to such State
 13 under subsection (e)(1).

14 (B) COORDINATION WITH CYBERSECURITY
 15 AND MODERNIZATION GRANTS.—The amount
 16 under subsection (e)(1) for purposes of grants
 17 under subsection (a)(1) to a State shall be re-
 18 duced by the amount of grants provided under
 19 this subsection to election agencies within the
 20 State, less any unused amount returned to the
 21 Department.

22 (g) INTERIM GRANT PROGRAM FOR NON-PAPER
 23 EQUIPMENT REPLACEMENT.—

24 (1) IN GENERAL.—The Secretary shall award
 25 grants to States designated under paragraph (2) for

1 the purpose of replacing voting systems that would
2 not be eligible for purchase under subsection (c)(3).

3 (2) ELIGIBILITY.—Not later than 60 days after
4 the date of enactment of this Act, the Secretary
5 shall develop a list of States in which 10 percent or
6 more of votes in the first Federal election occurring
7 after the date of enactment of this Act are expected
8 to be cast using voting systems that would not be el-
9 igible for purchase under subsection (c)(3), and shall
10 submit the list to the appropriate congressional com-
11 mittees.

12 (3) USE OF FUNDS.—A State election agency
13 that receives funds under paragraph (1) shall only
14 use the funds to replace voting systems that would
15 not be eligible for purchase under subsection (c)(3).

16 (4) APPLICATION PROCESS.—The Secretary
17 shall—

18 (A) establish an application process for
19 States designated under paragraph (2) to apply
20 for grants under this subsection; and

21 (B) consider the recommendations of the
22 Advisory Panel under section 5(c) in estab-
23 lishing the application process; and ensure that
24 a State applying for a grant submits—

1 (i) an inventory of voting systems in
 2 the State that would not be eligible for
 3 purchase under subsection(c)(3);

4 (ii) a plan to expeditiously replace
 5 those voting systems; and

6 (iii) a commitment to State funding
 7 for replacements that is at least equivalent
 8 to the grant amount.

9 (5) REVIEW.—The Secretary—

10 (A) shall fund a State application if the
 11 Secretary determines that the State will likely
 12 replace the voting systems that would not be el-
 13 igible for purchase under subsection (c)(3); and

14 (B) in reviewing a State application, shall
 15 consider the recommendations and criteria of
 16 the Advisory Panel under section 5(c).

17 (6) LIMITATIONS; COORDINATION WITH CYBER-
 18 SECURITY AND MODERNIZATION GRANTS.—

19 (A) LIMITATIONS.—Of the total amount
 20 authorized to be appropriated under subsection
 21 (i) for the first fiscal year beginning after the
 22 date of enactment of this Act, \$186,000,000
 23 shall be used for grants awarded under this
 24 subsection.

1 (B) FORMULA FOR GRANT AMOUNTS.—

2 The grant amount made available to each State
 3 shall be set according to the proportional for-
 4 mula described in subsection (e), as applied to
 5 the list of States designated under paragraph
 6 (2) and the number of votes cast in those
 7 States using voting systems that would not be
 8 eligible for purchase under subsection (c)(3).

9 (C) COORDINATION WITH CYBERSECURITY
 10 AND MODERNIZATION GRANTS.—If the Sec-
 11 retary determines that no additional State will
 12 receive a grant under this paragraph, the Sec-
 13 retary shall reallocate any amounts remaining
 14 under subparagraph (A) to the cybersecurity
 15 and modernization grant program established
 16 under this section.

17 (h) FINANCIAL ASSISTANCE FOR AUDITING EX-
 18 PENSES.—

19 (1) IN GENERAL.—The Secretary shall award
 20 grants to States that, in order to implement the
 21 guidelines established under section 5(b), inspect (by
 22 hand and not by device) a number of marked paper
 23 ballots in a Federal election that is greater than 5
 24 percent of the voting age population within the State

1 (in the case of national or statewide office) or dis-
2 trict covered by the election.

3 (2) APPLICATION PROCESS.—The Secretary
4 shall establish an application process for a State
5 that qualifies under paragraph (1) to apply for a
6 grant to reimburse its expenses associated with in-
7 specting (by hand and not by device) paper ballots
8 in excess of 5 percent of the voting age population
9 within the State (in the case of national or statewide
10 office) or district covered by the election.

11 (3) LOCAL GOVERNMENTS.—A State election
12 agency may authorize some or all other election
13 agencies within the State to apply for grants under
14 paragraph (1).

15 (4) TIMING; DISTRIBUTION.—The Secretary
16 shall award grants under this subsection on January
17 31, 2019, and every 2 years thereafter. If the
18 amount appropriated for carrying out this subsection
19 is insufficient to fund the grants, the Secretary shall
20 fund them according to the proportional formula de-
21 scribed in subsection (e), as applied to the States
22 seeking grants under this subsection and the number
23 of marked paper ballots that were inspected by hand
24 in excess of 5 percent of the voting age population

1 within the State (in the case of national or statewide
2 office) or district covered by the election.

3 (5) LIMITATION.—Of the total amount author-
4 ized to be appropriated under subsection (i),
5 \$5,000,000 shall be used for grants under this sub-
6 section.

7 (i) AUTHORIZATION OF APPROPRIATIONS.—

8 (1) IN GENERAL.—There is authorized to be
9 appropriated to the Department \$386,000,000 to
10 carry out this section for fiscal year 2018.

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

14 (3) FUNDING SOURCE.—

15 (A) DEFINITIONS.—In this paragraph—

16 (i) the terms “agency”, “closeout”,
17 and “Federal grant award” have the
18 meanings given those terms in section 2 of
19 the Grants Oversight and New Efficiency
20 Act (Public Law 114–117; 130 Stat. 6);
21 and

22 (ii) the term “Director” means the
23 Director of the Office of Management and
24 Budget.

1 (B) CLOSEOUT OF EXPIRED AND
2 UNDISBURSED FEDERAL GRANTS.—Not later
3 than 1 year after the date of enactment of this
4 Act, the Director shall promulgate procedures
5 requiring the head of each agency to promptly
6 conduct a closeout of each Federal grant award.

7 (C) RELATED REPORTS.—In promulgating
8 the procedures required under subparagraph
9 (B), the Director shall consider the rec-
10 ommendations and data in the reports required
11 to be submitted under section 2 of the Grants
12 Oversight and New Efficiency Act (Public Law
13 114–117; 130 Stat. 6) and section 530 of the
14 Commerce, Justice, Science, and Related Agen-
15 cies Appropriations Act, 2016 (Public Law
16 114–113; 129 Stat. 2329), and similar reports.

17 (D) EXPIRATION.—The procedures re-
18 quired under subparagraph (B) shall expire 4
19 years after the date on which the procedures
20 are promulgated.

21 **SEC. 8. HACK THE ELECTION PROGRAM.**

22 (a) ESTABLISHMENT.—Not later than 1 year after
23 the date of enactment of this Act, the Secretary shall es-
24 tablish a program to improve election system cybersecurity
25 by facilitating and encouraging assessments by inde-

1 pendent technical experts, in cooperation with election
2 agencies and election service providers, to identify and re-
3 port election cybersecurity vulnerabilities.

4 (b) VOLUNTARY PARTICIPATION.—Participation in
5 the Hack the Election program shall be entirely voluntary
6 for election agencies and election service providers.

7 (c) INPUT FROM ELECTION AGENCIES.—In devel-
8 oping the Hack the Election program under this section,
9 the Secretary shall solicit input from election agencies,
10 and shall encourage election agencies to participate.

11 (d) ACTIVITIES.—In establishing the program re-
12 quired under subsection (a), the Secretary shall—

13 (1) establish a recurring competition for inde-
14 pendent technical experts to assess election systems
15 for the purpose of identifying and reporting election
16 cybersecurity vulnerabilities;

17 (2) establish an expeditious process by which
18 independent technical experts can qualify to partici-
19 pate in the competition;

20 (3) establish a schedule of awards (monetary or
21 non-monetary) for reports of previously unidentified
22 election cybersecurity vulnerabilities discovered by
23 independent technical experts during the competi-
24 tion;

1 (4) establish a process for election agencies and
2 election service providers to voluntarily participate in
3 the program by designating specific election systems,
4 periods of time, and circumstances for assessment
5 by independent technical experts; and

6 (5) promptly notify election agencies and elec-
7 tion service providers about relevant election cyber-
8 security vulnerabilities discovered through the com-
9 petition, and provide technical assistance in rem-
10 edying the vulnerabilities.

11 (e) USE OF SERVICE PROVIDERS.—The Secretary
12 may award competitive contracts as necessary to manage
13 the program required under subsection (a).

14 (f) CONSULTATION.—In developing the program re-
15 quired under subsection (a), the Secretary shall consult
16 with—

17 (1) the Attorney General to address possible li-
18 ability for participating individuals under section
19 1030 of title 18, United States Code, section 1201
20 of title 17, United States Code, or other relevant
21 Federal law; and

22 (2) the relevant offices at the Department of
23 Defense that were responsible for launching the
24 2016 “Hack the Pentagon” pilot program and sub-

- 1 sequent Department of Defense bug bounty pro-
- 2 grams.

○