115TH CONGRESS
1ST SESSION

S. _____

To protect the administration of Federal elections against cybersecurity threats.

IN THE SENATE OF THE UNITED STATES

_____

_____ introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To protect the administration of Federal elections against cybersecurity threats.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Secure Elections Act''.

SEC. 2. SENSE OF CONGRESS.

It is the sense of Congress that—

(1) under the Constitution of the United States, the States conduct elections, and Congress recognizes the importance of maintaining State leadership in election administration;

(2) free and fair elections are central to our democracy;

(3) protecting our elections is a national security priority; and

(4) an attack on our election systems by a foreign power is a hostile act and should be met with appropriate retaliatory actions, including immediate and severe sanctions.

SEC. 3. DEFINITIONS.

In this Act:

(1) ADVISORY PANEL.—The term ''Advisory Panel'' means the advisory panel of independent experts on election cybersecurity established under section 5(a)(1).

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Rules and Administration, 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.

(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 such other elements of the intelligence community (as defined in section 3 of the National Se-

curity Act of 1947 (50 U.S.C. 3003)) as the Director of National Intelligence determines are appropriate.

(4) CHAIRMAN.—The term ''Chairman'' means the Chairman of the Election Assistance Commission.

(5) COMMISSION.—The term ''Commission'' means the Election Assistance Commission.

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

(7) 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.

(8) ELECTION CYBERSECURITY INCIDENT.—The term ''election cybersecurity incident'' means any information security incident involving an election system.

(9) 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.

(10) 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.

(11) 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.

(12) ELECTION SYSTEM.—The term ''election system'' means any information system (as defined in section 3502 of title 44, United States Code) used for the management, support, or administration of a Federal election, such as a voting system, a voter registration website or database, an electronic pollbook, a system for tabulating or reporting election results, or an election agency email system.

(13) FEDERAL ELECTION.—The term ''Federal election'' means any election (as defined in section 301(1) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(1)) for Federal office (as defined in section 301(3) of the Federal Election Campaign Act of 1971 (52 U.S.C. 30101(3)).

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

(15) INCIDENT.—The term ''incident'' has the meaning given the term in section 3552 of title 44, United States Code.

(16) INFORMATION SECURITY.—The term ''information security'' has the meaning given the term in section 3552 of title 44, United States Code.

(17) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security, or, upon designation by the Secretary of Homeland Security, the Deputy Secretary of Homeland Security, the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department, or a Senate-confirmed official that reports to that Under Secretary.

(18) 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.

(19) 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 designated by the State for purposes of this Act.

(20) STATE LAW ENFORCEMENT OFFICER.—The term ''State law enforcement officer'' means the head of a State law enforcement agency, such as an attorney general.

(21) 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. 4. 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) PRESUMPTION OF FEDERAL AND STATE INFORMATION SHARING FROM THE DEPARTMENT.—If the Department receives information about an election cybersecurity incident, threat, or vulnerability, unless the Secretary makes a specific determination in writing that there is good cause to withhold the particular information, the Department shall promptly share that information with—

(1) the appropriate Federal entities;

(2) all State election agencies;

(3) all election agencies that have requested ongoing updates on election cybersecurity incidents, threats, or vulnerabilities; and

(4) all election agencies that may be affected by the risks associated with the particular election cybersecurity incident, threat, or vulnerability.

(d) TECHNICAL RESOURCES FOR ELECTION AGENCIES.—In sharing information about election cybersecurity incidents, threats, and vulnerabilities with election agencies under this section, the Department shall, to the extent possible—

(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 protecting against and detecting associated risks;

(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.

(e) 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; and

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

(f) ROLE OF NON-FEDERAL ENTITIES.—The Department may share information about election cybersecurity incidents, threats, and vulnerabilities through a non-Federal entity, such as the Multi-State Information Sharing and Analysis Center.

(g) PROTECTION OF PERSONAL AND CONFIDENTIAL INFORMATION.—If a Federal entity shares information about an election cybersecurity incident, threat, or vulnerability, the Federal entity shall—

(1) minimize the acquisition, retention, 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; and

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

(h) 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 assess whether an election cybersecurity incident occurred and notify the State election official.

(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 assess whether an election cybersecurity incident occurred and notify the relevant election agencies consistent with subsection (j).

(i) 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 expedient time possible and without unreasonable delay (in no event longer than 3 calendar days after discovery of the incident), provide notification of the election cybersecurity incident to the Secretary.

(j) 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 information security 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 unreasonable delay (in no event longer than 3 calendar days after discovery of the possible incident); and

(2) cooperate with the election agencies in providing 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 cybersecurity incident, including the specific election 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

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

(l) 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.

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

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

(2) may create a classified annex to the catalog and make it available only to election agency personnel with appropriate security clearance.

(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 Chairman, 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 Multi-State 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 Chairman shall solicit and consider comments from all State election agencies.

(3) DISTRIBUTION.—The Secretary and the Chairman 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.—

(1) IN GENERAL.—If an appropriate Federal entity has reason to believe that a significant election cybersecurity incident has occurred, the entity shall—

(A) not later than 7 calendar days after the date on which there is a reasonable basis to conclude that the significant incident has occurred, provide notification of the incident to—

(i) the appropriate congressional committees;

(ii) the members of the Senate representing the States affected by the incident; and

(iii) the members of the House of Representatives representing the congressional districts affected by the incident; and

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

(2) REPORTING THRESHOLD.—The Secretary shall—

(A) promulgate a uniform definition of a ''significant election cybersecurity incident''; and

(B) shall submit the definition promulgated under subparagraph (A) to the appropriate congressional committees.

SEC. 5. ADVISORY PANEL AND GUIDELINES.

(a) ADVISORY PANEL.—

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

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

(A) 5 shall be appointed by the Secretary, in consultation with the Chairman and the Director of the National Institute of Standards and Technology, of whom 1 shall be designated as the Chairperson of the Advisory Panel;

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

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

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

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

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

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

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

(C) if appointed under any other subparagraph of paragraph (2), shall possess expertise in cybersecurity, election law, or election administration.

(4) TERMS; VACANCIES.—Members of the Advisory Panel shall serve for a term set by the Secretary. Any vacancy in the Advisory Panel shall be filled in the same manner as the original appointment.

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

compensation, except that members of the Advisory Panel may be allowed 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 Advisory Panel.

(6) ADMINISTRATIVE STAFF.—Upon request of the Advisory Panel, the Secretary shall provide to the Advisory Panel, on a reimbursable basis, the administrative support services necessary for the Advisory Panel to carry out its responsibilities under this Act.

(b) GUIDELINES.—

(1) IN GENERAL.—The Advisory Panel shall develop a set of guidelines for election cybersecurity, including standards for procuring, maintaining, testing, auditing, operating, and updating election systems.

(2) REQUIREMENTS.—In developing the guidelines, the Advisory Panel shall—

(A) identify the top risks to election systems;

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

(C) 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) GRANT PROGRAM.—The Advisory Panel shall assist the Department and the Commission in carrying out the grant program required under section 7 by—

(1) submitting recommendations to the Department about the grant program application process;

(2) submitting recommendations, including recommended criteria, to the Department for the grant program review process;

(3) submitting recommendations, including recommended criteria, to the Department for use of remaining grant funds;

(4) submitting recommendations, including recommended criteria, to the Department for the interim grant program for non-paper equipment replacement; and

(5) providing any other assistance that the Department or the Commission requests.

(d) PAPER BALLOTS AND STATISTICAL AUDITS.—The guidelines developed under subsection (b) shall include provisions regarding paper ballots and statistical audits for Federal elections, including that—

(1) each vote is made by a paper ballot (marked by hand or device), and the voter has an opportunity to inspect and confirm the marked paper ballot before casting it (consistent with accessibility accommodations); and

(2) each election result is determined by tabulating marked paper ballots (by hand or device), and prior to certification by a State of the election result, election agencies within the State inspect (by hand and not by device) a random sample of the marked paper ballots and thereby establish high statistical confidence in the election result.

(e) ISSUES CONSIDERED.—

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

(A) 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, re-

sponding to, and recovering from cybersecurity events;

(B) mechanisms to verify that election systems accurately tabulate ballots, report results, and identify a winner for each election for Federal office, even if computer hardware or software malfunctions due to error or an election cybersecurity incident;

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

(D) durational requirements needed to facilitate election audits prior to election certification, including variations in the acceptance of postal ballots, time allowed to cure provisional ballots, and election certification deadlines;

(E) providing actionable guidance to election agencies that have not applied for or received grant funds under section 7, and to agencies that seek to implement additional cybersecurity protections;

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

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

(2) RELATIONSHIP TO VOLUNTARY VOTING GUIDELINES AND NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CYBERSECURITY GUIDANCE.—In developing the guidelines required under subsection (b), the Advisory Panel shall consider—

(A) the Voluntary Voting Guidelines developed by the Commission; and

(B) 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)).

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

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

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

(g) CONSULTATION.—In developing the guidelines required under subsection (b), the Advisory Panel shall consult with—

(1) the appropriate Federal entities;

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

(3) the Federal Communications Commission;

(4) the Federal Trade Commission;

(5) the National Governors Association;

(6) the National Association of Secretaries of State;

(7) the National Association of State Election Directors;

(8) the National Association of Election Officials;

(9) the National Association of Counties;

(10) the National League of Cities;

(11) the International Association of Government Officials;

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

(13) the National Science Foundation; and

(14) any other interested entities that the Advisory Panel determines are necessary to the development of the guidelines.

(h) SUBMISSION TO SECRETARY.—Not later than 180 days after the date of enactment of this Act, the Advisory Panel shall submit the guidelines required under subsection (b) to the Secretary.

(i) SUBMISSION TO CONGRESS; MODIFICATION.—Not later than 14 calendar days after the date on which the Secretary receives guidelines under subsection (h) or (l), the Secretary shall submit the guidelines to the appropriate congressional committees. The Secretary may modify the guidelines in advance of submission to Congress if—

(1) the Secretary determines that there is good cause to modify the guidelines, consistent with the considerations established in subsection (f) and notwithstanding the recommendation of the Advisory Panel; and

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

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

subsection (b) to all election agencies known to the Department and the Commission.

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

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

(m) RULE OF CONSTRUCTION.—Nothing in the section shall be construed to subject the process for developing the guidelines required under subsection (b) to subchapter II of chapter 5, and chapter 7, of title 5, United States Code (commonly known as the ''Administrative Procedure Act'').

SEC. 6. REPORTS TO CONGRESS.

(a) REPORTS ON FOREIGN THREATS TO ELECTIONS.—

(1) 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 elec-

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

(2) 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.

(b) REPORTS ON GRANT PROGRAM.—Not later than 2 years after the date of enactment of this Act, and every 4 years thereafter, the Comptroller General of the United States shall submit a report to the appropriate congressional committees on the Department grant program established under section 7, including how grant funds have been distributed and used to implement the guidelines required under section 5(b).

SEC. 7. STATE ELECTION SYSTEM CYBERSECURITY AND MODERNIZATION GRANTS.

(a) AUTHORITY.—

(1) IN GENERAL.—The Secretary, acting through 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, shall award grants to States in accordance with this section.

(2) COORDINATION.—

(A) IN GENERAL.—The Secretary shall coordinate with the Commission in carrying out this section.

(B) JOINT PROGRAM.—If the Secretary determines that jointly carrying out this section with the Commission would increase State participation and cybersecurity preparedness, the Secretary shall—

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

(ii) enter into a Memorandum of Understanding with the Commission to carry out the grant program.

(b) APPLICATION PROCESS.—

(1) IN GENERAL.—The Secretary shall—

(A) establish a process for States to apply for election system cybersecurity and modernization grants;

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

(C) ensure that the application process requires that a State seeking a grant provide a detailed explanation of how election agencies within the State will implement the guidelines established under section 5(b).

(2) REVIEW.—The Secretary—

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

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

(ii) with respect to the guidelines related to statistical audits, consistent with section 5(d), the State will complete a statewide pilot program during a biennial Federal general election not later than 2022; and

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

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

(3) STATE IMPLEMENTATION.—

(A) IN GENERAL.—A State receiving a grant under this section may adopt any reasonable implementation of the guidelines established under section 5(b).

(B) INCONSISTENCY WITH STATE LAW.—If implementation of the guidelines would be inconsistent with State law, the State—

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

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

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

(4) PROTECTION OF PERSONAL INFORMATION.—The application process established under this subsection shall not require a State to disclose the personal information of any voter.

(c) USE OF FUNDS.—

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

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

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

(A) the State election official submits a written certification to the Secretary that the election agencies within the State have implemented the guidelines established under section 5(b); and

(B) the Secretary, after consideration of the recommendations and criteria of the Advisory Panel under section 5(c), approves the use of funds.

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

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

trator of General Services, in consultation with the Director of the National Institute of Standards and Technology, shall take such actions as may be necessary through competitive processes—

(1) to qualify a set of private sector entities that are capable of assisting the States with identifying, protecting against, detecting, responding to, and recovering from election cybersecurity incidents, threats, and vulnerabilities;

(2) to establish contract vehicles to enable States to access the services of 1 or more of the private sector organizations after receiving amounts under a grant under this section;

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

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

(e) LIMITATION ON AMOUNT OF GRANT.—

(1) IN GENERAL.—Subject to paragraph (3), the amount of funds provided to a State under a grant under this section shall be equal to the product obtained by multiplying—

(A) the total amount appropriated for grants pursuant to the authorization under section 6; by

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

(2) STATE ALLOCATION PERCENTAGE.—The State allocation percentage for a State is the amount (expressed as a percentage) equal to the quotient obtained by dividing—

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

(B) the voting age population of the State (as reported in the most recent decennial census).

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

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

(B) in the case of the Commonwealth of Puerto Rico, Guam, American Samoa, the Commonwealth of Northern Mariana Islands, or the

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

(4) PRO RATA REDUCTIONS.—The Secretary shall make such pro rata reductions to the allocations determined under paragraph (1) as are necessary to comply with the requirements of paragraph (3).

(f) INTERIM GRANT PROGRAM FOR ELECTION PREPAREDNESS.—

(1) IN GENERAL.—The Secretary shall award a grant to an election agency, regardless of State submission of an application under subsection (b), that—

(A) receives a ''cyber hygiene'' scan, a risk and vulnerability assessment, or a similar cybersecurity evaluation by the Department or a contractor approved by the Department; and

(B) not later than November 6, 2018, submits to the Department—

(i) the results of the evaluation described in subparagraph (A);

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

(iii) in the case of an application by any election agency of a political subdivision of a State, a certification of approval from the State election agency.

(2) PRIORITIZATION FOR LOCAL GOVERNMENTS.—A State election agency may authorize some or all other election agencies within the State to apply for interim grants under paragraph (1). If the amount available under paragraph (5) is not sufficient to fund the applications received from election agencies within the State, the State election agency may establish a priority order for funding applications.

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

(4) UNAVAILABILITY OF DEPARTMENT SERVICES.—If an election agency requests an evaluation by the Department consistent with paragraph (1)(A), and the Department is not able to provide the evaluation during the 30-calendar-day period following the request, the agency may—

(A) procure a reasonably equivalent evaluation from a private-sector entity; and

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

(5) LIMITATION ON AMOUNT OF GRANT; COORDINATION WITH CYBERSECURITY AND MODERNIZATION GRANTS.—

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

(B) COORDINATION WITH CYBERSECURITY AND MODERNIZATION GRANTS.—The amount under subsection (e)(1) for purposes of grants under subsection (a)(1) to a State shall be reduced by the amount of grants provided under this subsection to election agencies within the State, less any unused amount returned to the Department.

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

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

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

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

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

(4) APPLICATION PROCESS.—The Secretary shall—

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

(B) consider the recommendations of the Advisory Panel under section 5(c) in establishing the application process; and ensure that a State applying for a grant submits—

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

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

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

(5) REVIEW.—The Secretary—

(A) shall fund a State application if the Secretary determines that the State will likely replace the voting systems that would not be eligible for purchase under subsection (c)(3); and

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

(6) LIMITATIONS; COORDINATION WITH CYBERSECURITY AND MODERNIZATION GRANTS.—

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

(B) FORMULA FOR GRANT AMOUNTS.—The grant amount made available to each State shall be set according to the proportional formula described in subsection (e), as applied to the list of States designated under paragraph (2) and the number of votes cast in those States using voting systems that would not be eligible for purchase under subsection (c)(3).

(C) COORDINATION WITH CYBERSECURITY AND MODERNIZATION GRANTS.—If the Secretary determines that no additional State will receive a grant under this paragraph, the Secretary shall reallocate any amounts remaining under subparagraph (A) to the cybersecurity and modernization grant program established under this section.

(h) FINANCIAL ASSISTANCE FOR AUDITING EXPENSES.—

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

(in the case of national or statewide office) or district covered by the election.

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

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

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

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

(5) LIMITATION.—Of the total amount authorized to be appropriated under subsection (i), $5,000,000 shall be used for grants under this subsection.

(i) AUTHORIZATION OF APPROPRIATIONS.—

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

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

(3) FUNDING SOURCE.—

(A) DEFINITIONS.—In this paragraph—

(i) the terms ''agency'', ''closeout'', and ''Federal grant award'' have the meanings given those terms in section 2 of the Grants Oversight and New Efficiency Act (Public Law 114–117; 130 Stat. 6); and

(ii) the term ''Director'' means the Director of the Office of Management and Budget.

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

(C) RELATED REPORTS.—In promulgating the procedures required under subparagraph (B), the Director shall consider the recommendations and data in the reports required to be submitted under section 2 of the Grants Oversight and New Efficiency Act (Public Law 114–117; 130 Stat. 6) and section 530 of the Commerce, Justice, Science, and Related Agencies Appropriations Act, 2016 (Public Law 114–113; 129 Stat. 2329), and similar reports.

(D) EXPIRATION.—The procedures required under subparagraph (B) shall expire 4 years after the date on which the procedures are promulgated.

SEC. 8. HACK THE ELECTION PROGRAM.

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

pendent technical experts, in cooperation with election agencies and election service providers, to identify and report election cybersecurity vulnerabilities.

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

(c) INPUT FROM ELECTION AGENCIES.—In developing the Hack the Election program under this section, the Secretary shall solicit input from election agencies, and shall encourage election agencies to participate.

(d) ACTIVITIES.—In establishing the program required under subsection (a), the Secretary shall—

(1) establish a recurring competition for independent technical experts to assess election systems for the purpose of identifying and reporting election cybersecurity vulnerabilities;

(2) establish an expeditious process by which independent technical experts can qualify to participate in the competition;

(3) establish a schedule of awards (monetary or non-monetary) for reports of previously unidentified election cybersecurity vulnerabilities discovered by independent technical experts during the competition;

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

(5) promptly notify election agencies and election service providers about relevant election cybersecurity vulnerabilities discovered through the competition, and provide technical assistance in remedying the vulnerabilities.

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

(f) CONSULTATION.—In developing the program required under subsection (a), the Secretary shall consult with—

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

(2) the relevant offices at the Department of Defense that were responsible for launching the 2016 ''Hack the Pentagon'' pilot program and sub-

sequent Department of Defense bug bounty programs.