115TH CONGRESS
1ST SESSION

S. 516

To provide grants to assist States in developing and implementing plans to address cybersecurity threats or vulnerabilities, and for other purposes.

IN THE SENATE OF THE UNITED STATES

MARCH 2, 2017

Mr. WARNER (for himself and Mr. GARDNER) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

A BILL

To provide grants to assist States in developing and implementing plans to address cybersecurity threats or vulnerabilities, and for other purposes.

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 ''State Cyber Resiliency Act''.

SEC. 2. ESTABLISHMENT OF CYBER RESILIENCY GRANT PROGRAM.

(a) ESTABLISHMENT.—There is established the State Cyber Resiliency Grant Program to assist State, local, and

tribal governments in preventing, preparing for, protecting against, and responding to cyber threats, which shall be administered by the Administrator of the Federal Emergency Management Agency.

(b) ELIGIBILITY.—Each State shall be eligible to apply for grants under the Program.

(c) GRANTS AUTHORIZED FOR EACH STATE.—Subject to the funds available under a funding allocation determined under subsection (f) for a State, the Secretary of Homeland Security may award to the State—

(1) up to 2 planning grants under subsection (e) to develop or revise a cyber resiliency plan; and

(2) up to 2 implementation grants under subsection (f) to implement an active cyber resiliency plan.

(d) APPROVAL OF CYBER RESILIENCY PLANS.—

(1) IN GENERAL.—The Secretary shall approve a cyber resiliency plan submitted by a State if the Secretary determines, after considering the recommendations of the Review Committee established under subsection (i), that the plan meets all of the following criteria:

(A) The plan incorporates, to the extent practicable, any existing plans of such State to

protect against cybersecurity threats or vulnerabilities.

(B) The plan is designed to achieve each of the following objectives, with respect to the essential functions of such State:

(i) Enhancing the preparation, response, and resiliency of computer networks, industrial control systems, and communications systems performing such functions against cybersecurity threats or vulnerabilities.

(ii) Implementing a process of continuous cybersecurity vulnerability assessments and threat mitigation practices to prevent the disruption of such functions by an incident within the State.

(iii) Ensuring that entities performing such functions within the State adopt generally recognized best practices and methodologies with respect to cybersecurity, such as the practices provided in the cybersecurity framework developed by the National Institute of Standards and Technology.

(iv) Mitigating talent gaps in the State government cybersecurity workforce, enhancing recruitment and retention efforts for such workforce, and bolstering the knowledge, skills, and abilities of State government personnel to protect against cybersecurity threats and vulnerabilities.

(v) Protecting public safety answering points and other emergency communications and data networks from cybersecurity threats or vulnerabilities.

(vi) Ensuring continuity of communications and data networks between entities performing such functions within the State, in the event of a catastrophic disruption of such communications or networks.

(vii) Accounting for and mitigating, to the greatest degree possible, cybersecurity threats or vulnerabilities related to critical infrastructure or key resources, the degradation of which may impact the performance of such functions within the State or threaten public safety.

(viii) Providing appropriate communications capabilities to ensure cybersecurity intelligence information-sharing and the command and coordination capabilities among entities performing such functions.

(ix) Developing and coordinating strategies with respect to cybersecurity threats or vulnerabilities in consultation with—

(I) neighboring States or members of an information sharing and analysis organization; and

(II) as applicable, neighboring countries.

(2) DURATION OF APPROVAL.—

(A) INITIAL DURATION.—An approval under paragraph (1) shall be initially effective for the two-year period beginning on the date of the determination described in such paragraph.

(B) ANNUAL EXTENSION.—The Secretary may annually extend such approval for a one-year period, if the Secretary determines, after considering the recommendations of the Review Committee, that the plan continues to meet the criteria described in paragraph (1) after the

State makes such revisions as the Secretary may determine to be necessary.

(3) ESSENTIAL FUNCTIONS.—For purposes of this subsection, the term ''essential functions'' includes, with respect to a State, those functions that enhance the cybersecurity posture of the State, local and tribal governments of the State, and the public services they provide.

(e) PLANNING GRANTS.—

(1) INITIAL PLANNING GRANT.—The Secretary shall require, as a condition of awarding an initial planning grant, that the State seeking the grant—

(A) agrees to use the funds to develop a cyber resiliency plan designed to meet the criteria described in subsection (d)(1); and

(B) submits an application including such information as the Secretary may determine to be necessary.

(2) ELIGIBILITY FOR INITIAL PLANNING GRANT.—A State shall not be eligible to receive an initial planning grant after the date on which the State first submits a cyber resiliency plan to the Secretary for a determination under subsection (d)(1).

(3) ADDITIONAL PLANNING GRANT.—The Secretary may award an additional planning grant to a State if the State agrees to use the funds to revise a cyber resiliency plan in order to receive an extension in accordance with subsection (d)(2)(B), and submits an application including such information as the Secretary may determine to be necessary.

(4) LIMITATIONS ON NUMBER AND TIMING OF GRANTS.—A State shall not be eligible to receive—

(A) more than 2 planning grants under this subsection; or

(B) an additional planning grant for the fiscal year following the fiscal year for which it receives an initial planning grant.

(f) IMPLEMENTATION GRANTS.—

(1) APPLICATION REQUIREMENTS.—The Secretary shall require, as a condition of awarding a biennial implementation grant, that the State seeking the grant submits an application including the following:

(A) A proposal, including a description and timeline, of the activities to be funded by the grant as described by a cyber resiliency plan of the State approved under subsection (d).

(B) A description of how each activity proposed to be funded by the grant would achieve one or more of the objectives described in subsection (d)(1)(B).

(C) A description, if applicable, of how any prior biennial implementation grant awarded under this section was spent, and to what extent the criteria described in subsection (d)(1) were met.

(D) The share of any amounts awarded as a biennial implementation grant proposed to be distributed to local or tribal governments within such State.

(E) Such other information as the Secretary may determine to be necessary in consultation with the chief information officer, emergency managers, and senior public safety officials of the State.

(2) APPROVAL OF APPLICATION.—The Secretary shall consider the recommendations of the Review Committee in approving or disapproving an application for a biennial implementation grant.

(3) DISTRIBUTION TO LOCAL AND TRIBAL GOVERNMENTS.—

(A) IN GENERAL.—Not later than 45 days after the date that a biennial implementation grant is awarded, not less than 50 percent of any share proposed under paragraph (1)(D) shall be distributed to local or tribal governments, in the same manner that amounts awarded under section 2004 of the Homeland Security Act of 2002 (6 U.S.C. 605) are distributed to such governments, except that—

(i) no such distribution may be made to a federally recognized Indian tribe that is a State under subsection (k)(11)(B); and

(ii) in applying section 2004(c)(1) of such Act with respect to distributions under this subparagraph, ''100 percent'' shall be substituted for ''80 percent'' each place that term appears.

(B) CONSULTATION.—In determining how an implementation grant is distributed within a State, the State shall consult with local and regional chief information officer, emergency managers, and senior public safety officials of the State.

(4) COMPETITIVE AWARD.—Except as provided in subsection (h), biennial implementation grants shall be awarded—

(A) exclusively on a competitive basis; and

(B) based on the recommendations of the Review Committee.

(5) LIMITATION ON NUMBER OF GRANTS.—The Secretary may award to a State not more than 2 biennial implementation grants under this section.

(g) USE OF GRANT FUNDS.—

(1) LIMITATIONS.—Any grant awarded under this section shall supplement and not supplant State or local funds or, as applicable, funds supplied by the Bureau of Indian Affairs, and may not be used—

(A) to provide any Federal cost-sharing contribution on behalf of a State; or

(B) for any recreational or social purpose.

(2) APPROVED ACTIVITIES FOR IMPLEMENTATION GRANTS.—A State or a government entity that receives funds through a biennial implementation grant may use such funds for one or more of the following activities, to the extent that such activities are proposed under subsection (f)(1)(A):

(A) Supporting or enhancing information sharing and analysis organizations.

(B) Implementing or coordinating systems and services that use cyber threat indicators (as such term is defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501)) to address cybersecurity threats or vulnerabilities.

(C) Supporting dedicated cybersecurity and communications coordination planning, including the coordination of—

(i) emergency management elements of such State;

(ii) National Guard units, as appropriate;

(iii) entities associated with critical infrastructure or key resources;

(iv) information sharing and analysis organizations;

(v) public safety answering points; or

(vi) nongovernmental organizations engaged in cybersecurity research as a formally designated information analysis and sharing organization.

(D) Establishing programs, such as scholarships or apprenticeships, to provide financial assistance to State residents who—

(i) pursue formal education, training, and industry-recognized certifications for careers in cybersecurity as identified by the National Initiative for Cybersecurity Education; and

(ii) commit to working for State government for a specified period of time.

(h) FUNDING ALLOCATIONS.—

(1) IN GENERAL.—From any amount appropriated for a fiscal year that is not reserved for use by the Secretary in carrying out this section, the Secretary shall allocate the entire amount among the States (including the District of Columbia) eligible for grants under this section taking into consideration the factors specified in paragraph (2) and consistent with the following:

(A) ALLOCATIONS FOR THE SEVERAL STATES.—Of the amount subject to allocation, a funding allocation for any of such States shall be—

(i) not less than 0.001 percent, with respect to an initial planning grant, and

not more than 0.001 percent, with respect to any additional planning grants; and

(ii) not less than 0.5 percent and not more than 3 percent, with respect to biennial implementation grants.

(B) ALLOCATIONS FOR THE TERRITORIES AND POSSESSIONS.—Of the amount subject to allocation, a funding allocation for any of the territories and possessions of the United States eligible for grants under this section shall be—

(i) not less than 0.001 percent, with respect to an initial planning grant, and not more than 0.001 percent, with respect to any additional planning grant; and

(ii) not less than 0.1 percent and not more than 1 percent, with respect to biennial implementation grants.

(2) CONSIDERATIONS FOR FUNDING ALLOCATIONS.—In determining a funding allocation under paragraph (1) for a State, the Secretary shall consider each of the following factors:

(A) The considerations described in section 1809(h)(1) of the Homeland Security Act of 2002 (6 U.S.C. 579(h)(1)) with respect to the State, and the degree of exposure of the State

and protected government entities within the State to threats, vulnerabilities, or consequences resulting from cybersecurity risks or incidents.

(B) The degree of exposure of the State and protected government entities within the State to threats, vulnerabilities, or consequences resulting from cybersecurity risks or incidents.

(C) The effectiveness of, relative to evolving cyber threats against, cybersecurity assets, secure communications capabilities, and data network protections, of the State and its partners.

(D) The extent to which the State is vulnerable to cyber threats because it has not implemented best practices such as the cybersecurity framework developed by the National Institute of Standards and Technology.

(E) The extent to which a State government may face low cybersecurity workforce supply and high cybersecurity workforce demand, as identified by the National Institute of Standards and Technology

(i) REVIEW COMMITTEE FOR CYBER RESILIENCY GRANTS.—

(1) ESTABLISHMENT.—There is established a committee to be known as the ''Review Committee for Cyber Resiliency Grants'' (in this section referred to as the ''Review Committee'').

(2) CONSIDERATION OF SUBMISSIONS.—The Secretary shall forward a copy of each cyber resiliency plan submitted for approval under subsection (d)(1), each application for an additional planning grant submitted under subsection (e)(3), and each application for a biennial implementation grant submitted under subsection (d)(1) to the Review Committee for consideration under this subsection.

(3) DUTIES.—The Review Committee shall—

(A) promulgate guidance for the development of applications for grants under this section;

(B) review any plan or application forwarded under paragraph (2);

(C) provide to the State and to the Secretary the recommendations of the Review Committee regarding the approval or disapproval of such plan or application and, if applicable, possible improvements to such plan or application;

(D) provide to the Secretary an evaluation of any progress made by a State in imple-

menting an active cyber resiliency plan using a prior biennial implementation grant; and

(E) submit to Congress an annual report on the progress made in implementing active cyber resiliency plans.

(4) MEMBERSHIP.—

(A) NUMBER AND APPOINTMENT.—The Review Committee shall be composed of 15 members appointed by the Secretary as follows:

(i) At least 2 individuals recommended to the Secretary by the National Governors Association.

(ii) At least 1 individual recommended to the Secretary by the National Association of State Chief Information Officers.

(iii) At least 1 individual recommended to the Secretary by the National Guard Bureau.

(iv) At least 1 individual recommended to the Secretary by the National Association of Counties.

(v) At least 1 individual recommended to the Secretary by the National League of Cities.

(vi) Not more than 9 other individuals who have educational and professional experience related to cybersecurity analysis or policy.

(B) TERMS.—Each member shall be appointed for a term of one year. Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of that term. A member may serve after the expiration of that member's term until a successor has taken office. A vacancy in the Commission shall be filled in the manner in which the original appointment was made.

(C) PAY.—Members shall serve without pay.

(D) CHAIRPERSON; VICE CHAIRPERSON.—The Secretary, or a designee of the Secretary, shall serve as the Chairperson of the Review Committee. The Administrator of the Federal Emergency Management Agency, or a designee of the Administrator, shall serve as the Vice Chairperson of the Review Committee.

(5) STAFF AND EXPERTS.—The Review Committee may—

(A) appoint additional personnel as it considers appropriate, without regard to the provisions of title 5, United States Code, governing appointments in the competitive service;

(B) fix the pay of such additional personnel, without regard to the provisions of chapter 51 and subchapter III of chapter 53 of such title relating to classification and General Schedule pay rates; and

(C) procure temporary and intermittent services under section 3109(b) of such title.

(6) DETAILEES.—Upon request of the Review Committee, the head of any Federal department or agency may detail, on a reimbursable basis, any of the personnel of that department or agency to the Commission to assist it in carrying out the duties under this Act.

(7) FEDERAL ADVISORY COMMITTEE ACT.—The Federal Advisory Committee Act (5 U.S.C. App.) shall not apply to the Review Committee.

(8) TERMINATION.—The authority of the Review Committee shall terminate on the day after the

end of the five-fiscal-year period described in subsection (c).

(j) FUNDING.—There is authorized to be appropriated for grants under this section such sums as are necessary for fiscal years 2018 through 2023.

(k) DEFINITIONS.—In this section:

(1) ACTIVE CYBER RESILIENCY PLAN.—The term ''active cyber resiliency plan'' means a cyber resiliency plan for which an approval is in effect in accordance with subsection (d)(2)(A) or for which the Secretary extends such approval in accordance with subsection (d)(2)(B).

(2) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Federal Emergency Management Agency.

(3) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(4) CYBER RESILIENCY PLAN.—The term ''cyber resiliency plan'' means, with respect to a State, a plan that addresses the cybersecurity threats or vulnerabilities faced by the State through a statewide plan and decisionmaking process to respond to cybersecurity risks or incidents.

(5) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given that term in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148).

(6) INCIDENT.—The term ''incident'' has the meaning given that term in section 227 of the Homeland Security Act of 2002 (6 U.S.C. 148).

(7) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term ''information sharing and analysis organization'' has the meaning given that term in section 212 of the Homeland Security Act of 2002 (6 U.S.C. 131).

(8) KEY RESOURCES.—The term ''key resources'' has the meaning given that term in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(9) PROGRAM.—The term ''Program'' means the State Cyber Resiliency Grant Program established by this section.

(10) PUBLIC SAFETY ANSWERING POINTS.—The term ''public safety answering points'' has the meaning given that term in section 222(h) of the Communications Act of 1934 (47 U.S.C. 222(h)).

(11) STATE.—The term ''State''—

(A) means each of the several States, the District of Colombia, and the territories and possessions of the United States; and

(B) includes any federally recognized Indian tribe that notifies the Secretary, not later than 120 days after the date of the enactment of this Act or not later than 120 days before the start of any fiscal year during the five-fiscal-year period described in subsection (c), that the tribe intends to develop a cyber resiliency plan and agrees to forfeit any distribution under subsection (f)(3).

○