

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.

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 “State Cyber Resiliency
5 Act”.

6 **SEC. 2. ESTABLISHMENT OF CYBER RESILIENCY GRANT**
7 **PROGRAM.**

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

1 tribal governments in preventing, preparing for, protecting
2 against, and responding to cyber threats, which shall be
3 administered by the Administrator of the Federal Emer-
4 gency Management Agency.

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

7 (c) GRANTS AUTHORIZED FOR EACH STATE.—Sub-
8 ject to the funds available under a funding allocation de-
9 termined under subsection (f) for a State, the Secretary
10 of Homeland Security may award to the State—

11 (1) up to 2 planning grants under subsection

12 (e) to develop or revise a cyber resiliency plan; and

13 (2) up to 2 implementation grants under sub-
14 section (f) to implement an active cyber resiliency
15 plan.

16 (d) APPROVAL OF CYBER RESILIENCY PLANS.—

17 (1) IN GENERAL.—The Secretary shall approve
18 a cyber resiliency plan submitted by a State if the
19 Secretary determines, after considering the rec-
20 ommendations of the Review Committee established
21 under subsection (i), that the plan meets all of the
22 following criteria:

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

1 protect against cybersecurity threats or
2 vulnerabilities.

3 (B) The plan is designed to achieve each of
4 the following objectives, with respect to the es-
5 sential functions of such State:

6 (i) Enhancing the preparation, re-
7 sponse, and resiliency of computer net-
8 works, industrial control systems, and com-
9 munications systems performing such func-
10 tions against cybersecurity threats or
11 vulnerabilities.

12 (ii) Implementing a process of contin-
13 uous cybersecurity vulnerability assess-
14 ments and threat mitigation practices to
15 prevent the disruption of such functions by
16 an incident within the State.

17 (iii) Ensuring that entities performing
18 such functions within the State adopt gen-
19 erally recognized best practices and meth-
20 odologies with respect to cybersecurity,
21 such as the practices provided in the cyber-
22 security framework developed by the Na-
23 tional Institute of Standards and Tech-
24 nology.

1 (iv) Mitigating talent gaps in the
2 State government cybersecurity workforce,
3 enhancing recruitment and retention ef-
4 forts for such workforce, and bolstering the
5 knowledge, skills, and abilities of State
6 government personnel to protect against
7 cybersecurity threats and vulnerabilities.

8 (v) Protecting public safety answering
9 points and other emergency communica-
10 tions and data networks from cybersecurity
11 threats or vulnerabilities.

12 (vi) Ensuring continuity of commu-
13 nications and data networks between enti-
14 ties performing such functions within the
15 State, in the event of a catastrophic dis-
16 ruption of such communications or net-
17 works.

18 (vii) Accounting for and mitigating, to
19 the greatest degree possible, cybersecurity
20 threats or vulnerabilities related to critical
21 infrastructure or key resources, the deg-
22 radation of which may impact the perform-
23 ance of such functions within the State or
24 threaten public safety.

1 (viii) Providing appropriate commu-
 2 nications capabilities to ensure cybersecu-
 3 rity intelligence information-sharing and
 4 the command and coordination capabilities
 5 among entities performing such functions.

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

10 (I) neighboring States or mem-
 11 bers of an information sharing and
 12 analysis organization; and

13 (II) as applicable, neighboring
 14 countries.

15 (2) DURATION OF APPROVAL.—

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

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

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

3 (3) ESSENTIAL FUNCTIONS.—For purposes of
 4 this subsection, the term “essential functions” in-
 5 cludes, with respect to a State, those functions that
 6 enhance the cybersecurity posture of the State, local
 7 and tribal governments of the State, and the public
 8 services they provide.

9 (e) PLANNING GRANTS.—

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

13 (A) agrees to use the funds to develop a
 14 cyber resiliency plan designed to meet the cri-
 15 teria described in subsection (d)(1); and

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

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

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

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

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

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

15 (f) IMPLEMENTATION GRANTS.—

16 (1) APPLICATION REQUIREMENTS.—The Sec-
 17 retary shall require, as a condition of awarding a bi-
 18 ennial implementation grant, that the State seeking
 19 the grant submits an application including the fol-
 20 lowing:

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

1 (B) A description of how each activity pro-
 2 posed to be funded by the grant would achieve
 3 one or more of the objectives described in sub-
 4 section (d)(1)(B).

5 (C) A description, if applicable, of how any
 6 prior biennial implementation grant awarded
 7 under this section was spent, and to what ex-
 8 tent the criteria described in subsection (d)(1)
 9 were met.

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

14 (E) Such other information as the Sec-
 15 retary may determine to be necessary in con-
 16 sultation with the chief information officer,
 17 emergency managers, and senior public safety
 18 officials of the State.

19 (2) APPROVAL OF APPLICATION.—The Sec-
 20 retary shall consider the recommendations of the Re-
 21 view Committee in approving or disapproving an ap-
 22 plication for a biennial implementation grant.

23 (3) DISTRIBUTION TO LOCAL AND TRIBAL GOV-
 24 ERNMENTS.—

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

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

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

19 (B) CONSULTATION.—In determining how
20 an implementation grant is distributed within a
21 State, the State shall consult with local and re-
22 gional chief information officer, emergency
23 managers, and senior public safety officials of
24 the State.

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

4 (A) exclusively on a competitive basis; and
5 (B) based on the recommendations of the
6 Review Committee.

7 (5) LIMITATION ON NUMBER OF GRANTS.—The
8 Secretary may award to a State not more than 2 bi-
9 ennial implementation grants under this section.

10 (g) USE OF GRANT FUNDS.—

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

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

18 (B) for any recreational or social purpose.

19 (2) APPROVED ACTIVITIES FOR IMPLEMENTA-
20 TION GRANTS.—A State or a government entity that
21 receives funds through a biennial implementation
22 grant may use such funds for one or more of the fol-
23 lowing activities, to the extent that such activities
24 are proposed under subsection (f)(1)(A):

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

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

9 (C) Supporting dedicated cybersecurity
10 and communications coordination planning, in-
11 cluding the coordination of—

12 (i) emergency management elements
13 of such State;

14 (ii) National Guard units, as appro-
15 priate;

16 (iii) entities associated with critical in-
17 frastructure or key resources;

18 (iv) information sharing and analysis
19 organizations;

20 (v) public safety answering points; or

21 (vi) nongovernmental organizations
22 engaged in cybersecurity research as a for-
23 mally designated information analysis and
24 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

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

3 (ii) not less than 0.5 percent and not
4 more than 3 percent, with respect to bien-
5 nial implementation grants.

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

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

15 (ii) not less than 0.1 percent and not
16 more than 1 percent, with respect to bien-
17 nial implementation grants.

18 (2) CONSIDERATIONS FOR FUNDING ALLOCA-
19 TIONS.—In determining a funding allocation under
20 paragraph (1) for a State, the Secretary shall con-
21 sider each of the following factors:

22 (A) The considerations described in section
23 1809(h)(1) of the Homeland Security Act of
24 2002 (6 U.S.C. 579(h)(1)) with respect to the
25 State, and the degree of exposure of the State

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

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

8 (C) The effectiveness of, relative to evol-
 9 ving cyber threats against, cybersecurity assets,
 10 secure communications capabilities, and data
 11 network protections, of the State and its part-
 12 ners.

13 (D) The extent to which the State is vul-
 14 nerable to cyber threats because it has not im-
 15 plemented best practices such as the cybersecu-
 16 rity framework developed by the National Insti-
 17 tute of Standards and Technology.

18 (E) The extent to which a State govern-
 19 ment may face low cybersecurity workforce sup-
 20 ply and high cybersecurity workforce demand,
 21 as identified by the National Institute of Stand-
 22 ards and Technology

23 (i) REVIEW COMMITTEE FOR CYBER RESILIENCY
 24 GRANTS.—

1 (1) ESTABLISHMENT.—There is established a
2 committee to be known as the “Review Committee
3 for Cyber Resiliency Grants” (in this section re-
4 ferred to as the “Review Committee”).

5 (2) CONSIDERATION OF SUBMISSIONS.—The
6 Secretary shall forward a copy of each cyber resil-
7 iency plan submitted for approval under subsection
8 (d)(1), each application for an additional planning
9 grant submitted under subsection (e)(3), and each
10 application for a biennial implementation grant sub-
11 mitted under subsection (d)(1) to the Review Com-
12 mittee for consideration under this subsection.

13 (3) DUTIES.—The Review Committee shall—

14 (A) promulgate guidance for the develop-
15 ment of applications for grants under this sec-
16 tion;

17 (B) review any plan or application for-
18 warded under paragraph (2);

19 (C) provide to the State and to the Sec-
20 retary the recommendations of the Review Com-
21 mittee regarding the approval or disapproval of
22 such plan or application and, if applicable, pos-
23 sible improvements to such plan or application;

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

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

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

6 (4) MEMBERSHIP.—

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

10 (i) At least 2 individuals rec-
11 ommended to the Secretary by the Na-
12 tional Governors Association.

13 (ii) At least 1 individual recommended
14 to the Secretary by the National Associa-
15 tion of State Chief Information Officers.

16 (iii) At least 1 individual rec-
17 ommended to the Secretary by the Na-
18 tional Guard Bureau.

19 (iv) At least 1 individual rec-
20 ommended to the Secretary by the Na-
21 tional Association of Counties.

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

1 (vi) Not more than 9 other individuals
2 who have educational and professional ex-
3 perience related to cybersecurity analysis
4 or policy.

5 (B) TERMS.—Each member shall be ap-
6 pointed for a term of one year. Any member ap-
7 pointed to fill a vacancy occurring before the
8 expiration of the term for which the member's
9 predecessor was appointed shall be appointed
10 only for the remainder of that term. A member
11 may serve after the expiration of that member's
12 term until a successor has taken office. A va-
13 cancy in the Commission shall be filled in the
14 manner in which the original appointment was
15 made.

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

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

1 (5) STAFF AND EXPERTS.—The Review Com-
2 mittee may—

3 (A) appoint additional personnel as it con-
4 siders appropriate, without regard to the provi-
5 sions of title 5, United States Code, governing
6 appointments in the competitive service;

7 (B) fix the pay of such additional per-
8 sonnel, without regard to the provisions of
9 chapter 51 and subchapter III of chapter 53 of
10 such title relating to classification and General
11 Schedule pay rates; and

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

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

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

23 (8) TERMINATION.—The authority of the Re-
24 view Committee shall terminate on the day after the

1 end of the five-fiscal-year period described in sub-
2 section (c).

3 (j) FUNDING.—There is authorized to be appro-
4 priated for grants under this section such sums as are nec-
5 essary for fiscal years 2018 through 2023.

6 (k) DEFINITIONS.—In this section:

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

13 (2) ADMINISTRATOR.—The term “Adminis-
14 trator” means the Administrator of the Federal
15 Emergency Management Agency.

16 (3) CRITICAL INFRASTRUCTURE.—The term
17 “critical infrastructure” has the meaning given that
18 term in section 2 of the Homeland Security Act of
19 2002 (6 U.S.C. 101).

20 (4) CYBER RESILIENCY PLAN.—The term
21 “cyber resiliency plan” means, with respect to a
22 State, a plan that addresses the cybersecurity
23 threats or vulnerabilities faced by the State through
24 a statewide plan and decisionmaking process to re-
25 spond to cybersecurity risks or incidents.

1 (5) CYBERSECURITY RISK.—The term “cyberse-
2 curity risk” has the meaning given that term in sec-
3 tion 227 of the Homeland Security Act of 2002 (6
4 U.S.C. 148).

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

8 (7) INFORMATION SHARING AND ANALYSIS OR-
9 GANIZATION.—The term “information sharing and
10 analysis organization” has the meaning given that
11 term in section 212 of the Homeland Security Act
12 of 2002 (6 U.S.C. 131).

13 (8) KEY RESOURCES.—The term “key re-
14 sources” has the meaning given that term in section
15 2 of the Homeland Security Act of 2002 (6 U.S.C.
16 101).

17 (9) PROGRAM.—The term “Program” means
18 the State Cyber Resiliency Grant Program estab-
19 lished by this section.

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

24 (11) STATE.—The term “State”—

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

4 (B) includes any federally recognized In-
5 dian tribe that notifies the Secretary, not later
6 than 120 days after the date of the enactment
7 of this Act or not later than 120 days before
8 the start of any fiscal year during the five-fis-
9 cal-year period described in subsection (c), that
10 the tribe intends to develop a cyber resiliency
11 plan and agrees to forfeit any distribution
12 under subsection (f)(3).

○