

116TH CONGRESS
1ST SESSION

S. 1065

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

APRIL 8, 2019

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.

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

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

10 (1) up to 2 planning grants under subsection

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

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

15 (d) APPROVAL OF CYBER RESILIENCY PLANS.—

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

22 (A) The plan incorporates, to the extent
23 practicable, any existing plans of such State to
24 protect against cybersecurity threats or
25 vulnerabilities.

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

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

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

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

23 (iv) Mitigating talent gaps in the
24 State government cybersecurity workforce,
25 enhancing recruitment and retention ef-

1 forts for such workforce, and bolstering the
2 knowledge, skills, and abilities of State
3 government personnel to protect against
4 cybersecurity threats and vulnerabilities.

5 (v) Protecting public safety answering
6 points and other emergency communica-
7 tions and data networks from cybersecurity
8 threats or vulnerabilities.

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

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

22 (viii) Providing appropriate commu-
23 nications capabilities to ensure cybersecu-
24 rity intelligence information-sharing and

1 the command and coordination capabilities
2 among entities performing such functions.

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

7 (I) neighboring States or mem-
8 bers of an information sharing and
9 analysis organization; and

10 (II) as applicable, neighboring
11 countries.

12 (2) DURATION OF APPROVAL.—

13 (A) INITIAL DURATION.—An approval
14 under paragraph (1) shall be initially effective
15 for the 2-year period beginning on the date of
16 the determination described in such paragraph.

17 (B) ANNUAL EXTENSION.—The Secretary
18 may annually extend such approval for a 1-year
19 period, if the Secretary determines, after con-
20 sidering the recommendations of the Review
21 Committee, that the plan continues to meet the
22 criteria described in paragraph (1) after the
23 State makes such revisions as the Secretary
24 may determine to be necessary.

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

7 (e) PLANNING GRANTS.—

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

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

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

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

23 (3) ADDITIONAL PLANNING GRANT.—The Sec-
24 retary may award an additional planning grant to a
25 State if the State agrees to use the funds to revise

1 a cyber resiliency plan in order to receive an exten-
 2 sion in accordance with subsection (d)(2)(B), and
 3 submits an application including such information as
 4 the Secretary may determine to be necessary.

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

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

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

12 (f) IMPLEMENTATION GRANTS.—

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

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

22 (B) A description of how each activity pro-
 23 posed to be funded by the grant would achieve
 24 one or more of the objectives described in sub-
 25 section (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 govern-

ments, 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.

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

4 (g) USE OF GRANT FUNDS.—

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

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

12 (B) for any recreational or social purpose.

13 (2) APPROVED ACTIVITIES FOR IMPLEMENTA-
 14 TION GRANTS.—A State or a government entity that
 15 receives funds through a biennial implementation
 16 grant may use such funds for one or more of the fol-
 17 lowing activities, to the extent that such activities
 18 are proposed under subsection (f)(1)(A):

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

21 (B) Implementing or coordinating systems
 22 and services that use cyber threat indicators (as
 23 such term is defined in section 102 of the Cy-
 24 bersecurity Information Sharing Act of 2015 (6

1 U.S.C. 1501)) to address cybersecurity threats
2 or vulnerabilities.

3 (C) Supporting dedicated cybersecurity
4 and communications coordination planning, in-
5 cluding the coordination of—

6 (i) emergency management elements
7 of such State;

8 (ii) National Guard units, as appro-
9 priate;

10 (iii) entities associated with critical in-
11 frastructure or key resources;

12 (iv) information sharing and analysis
13 organizations;

14 (v) public safety answering points; or

15 (vi) nongovernmental organizations
16 engaged in cybersecurity research as a for-
17 mally designated information analysis and
18 sharing organization.

19 (D) Establishing programs, such as schol-
20 arships or apprenticeships, to provide financial
21 assistance to State residents who—

22 (i) pursue formal education, training,
23 and industry-recognized certifications for
24 careers in cybersecurity as identified by the

1 National Initiative for Cybersecurity Edu-
2 cation; and

3 (ii) commit to working for State gov-
4 ernment for a specified period of time.

5 (h) FUNDING ALLOCATIONS.—

6 (1) IN GENERAL.—From any amount appro-
7 priated for a fiscal year that is not reserved for use
8 by the Secretary in carrying out this section, the
9 Secretary shall allocate the entire amount among the
10 States (including the District of Columbia) eligible
11 for grants under this section taking into consider-
12 ation the factors specified in paragraph (2) and con-
13 sistent with the following:

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

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

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

1 (B) ALLOCATIONS FOR THE TERRITORIES

2 AND POSSESSIONS.—Of the amount subject to
3 allocation, a funding allocation for any of the
4 territories and possessions of the United States
5 eligible for grants under this section shall be—

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

10 (ii) not less than 0.1 percent and not
11 more than 1 percent, with respect to bien-
12 nial implementation grants.

13 (2) CONSIDERATIONS FOR FUNDING ALLOCA-

14 TIONS.—In determining a funding allocation under
15 paragraph (1) for a State, the Secretary shall con-
16 sider each of the following factors:

17 (A) The considerations described in section
18 1809(h)(1) of the Homeland Security Act of
19 2002 (6 U.S.C. 579(h)(1)) with respect to the
20 State, and the degree of exposure of the State
21 and protected government entities within the
22 State to threats, vulnerabilities, or consequences
23 resulting from cybersecurity risks or incidents.

24 (B) The degree of exposure of the State
25 and protected government entities within the

1 State to threats, vulnerabilities, or consequences
 2 resulting from cybersecurity risks or incidents.

3 (C) The effectiveness of, relative to evolving
 4 cyber threats against, cybersecurity assets,
 5 secure communications capabilities, and data
 6 network protections, of the State and its part-
 7 ners.

8 (D) The extent to which the State is vul-
 9 nerable to cyber threats because it has not im-
 10 plemented best practices such as the cybersecu-
 11 rity framework developed by the National Insti-
 12 tute of Standards and Technology.

13 (E) The extent to which a State govern-
 14 ment may face low cybersecurity workforce sup-
 15 ply and high cybersecurity workforce demand,
 16 as identified by the National Institute of Stand-
 17 ards and Technology.

18 (i) REVIEW COMMITTEE FOR CYBER RESILIENCY
 19 GRANTS.—

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

24 (2) CONSIDERATION OF SUBMISSIONS.—The
 25 Secretary shall forward a copy of each cyber resil-

1 iency plan submitted for approval under subsection
2 (d)(1), each application for an additional planning
3 grant submitted under subsection (e)(3), and each
4 application for a biennial implementation grant sub-
5 mitted under subsection (d)(1) to the Review Com-
6 mittee for consideration under this subsection.

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

8 (A) promulgate guidance for the develop-
9 ment of applications for grants under this sec-
10 tion;

11 (B) review any plan or application for-
12 warded under paragraph (2);

13 (C) provide to the State and to the Sec-
14 retary the recommendations of the Review Com-
15 mittee regarding the approval or disapproval of
16 such plan or application and, if applicable, pos-
17 sible improvements to such plan or application;

18 (D) provide to the Secretary an evaluation
19 of any progress made by a State in imple-
20 menting an active cyber resiliency plan using a
21 prior biennial implementation grant; and

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

25 (4) MEMBERSHIP.—

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

4 (i) At least 2 individuals rec-
5 ommended to the Secretary by the Na-
6 tional Governors Association.

7 (ii) At least 1 individual recommended
8 to the Secretary by the National Associa-
9 tion of State Chief Information Officers.

10 (iii) At least 1 individual rec-
11 ommended to the Secretary by the Na-
12 tional Guard Bureau.

13 (iv) At least 1 individual rec-
14 ommended to the Secretary by the Na-
15 tional Association of Counties.

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

19 (vi) Not more than 9 other individuals
20 who have educational and professional ex-
21 perience related to cybersecurity analysis
22 or policy.

23 (B) TERMS.—Each member shall be ap-
24 pointed for a term of 1 year. Any member ap-
25 pointed to fill a vacancy occurring before the

1 expiration of the term for which the member's
2 predecessor was appointed shall be appointed
3 only for the remainder of that term. A member
4 may serve after the expiration of that member's
5 term until a successor has taken office. A va-
6 cancy in the Commission shall be filled in the
7 manner in which the original appointment was
8 made.

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

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

18 (5) STAFF AND EXPERTS.—The Review Com-
19 mittee may—

20 (A) appoint additional personnel as it con-
21 sidered appropriate, without regard to the provi-
22 sions of title 5, United States Code, governing
23 appointments in the competitive service;

24 (B) fix the pay of such additional per-
25 sonnel, without regard to the provisions of

1 chapter 51 and subchapter III of chapter 53 of
 2 such title relating to classification and General
 3 Schedule pay rates; and

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

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

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

15 (8) TERMINATION.—The authority of the Re-
 16 view Committee shall terminate on the day after the
 17 end of the 5-fiscal-year period described in sub-
 18 section (j).

19 (j) FUNDING.—There is authorized to be appro-
 20 priated for grants under this section such sums as are nec-
 21 essary for fiscal years 2020 through 2025.

22 (k) DEFINITIONS.—In this section:

23 (1) ACTIVE CYBER RESILIENCY PLAN.—The
 24 term “active cyber resiliency plan” means a cyber
 25 resiliency plan for which an approval is in effect in

1 accordance with subsection (d)(2)(A) or for which
2 the Secretary extends such approval in accordance
3 with subsection (d)(2)(B).

4 (2) ADMINISTRATOR.—The term “Adminis-
5 trator” means the Administrator of the Federal
6 Emergency Management Agency.

7 (3) CRITICAL INFRASTRUCTURE.—The term
8 “critical infrastructure” has the meaning given that
9 term in section 2 of the Homeland Security Act of
10 2002 (6 U.S.C. 101).

11 (4) CYBER RESILIENCY PLAN.—The term
12 “cyber resiliency plan” means, with respect to a
13 State, a plan that addresses the cybersecurity
14 threats or vulnerabilities faced by the State through
15 a statewide plan and decisionmaking process to re-
16 spond to cybersecurity risks or incidents.

17 (5) CYBERSECURITY RISK.—The term “cyberse-
18 curity risk” has the meaning given that term in sec-
19 tion 2209 of the Homeland Security Act of 2002 (6
20 U.S.C. 659).

21 (6) INCIDENT.—The term “incident” has the
22 meaning given that term in section 2209 of the
23 Homeland Security Act of 2002 (6 U.S.C. 659).

24 (7) INFORMATION SHARING AND ANALYSIS OR-
25 GANIZATION.—The term “information sharing and

1 analysis organization” has the meaning given that
2 term in section 2222 of the Homeland Security Act
3 of 2002 (6 U.S.C. 671).

4 (8) KEY RESOURCES.—The term “key re-
5 sources” has the meaning given that term in section
6 2 of the Homeland Security Act of 2002 (6 U.S.C.
7 101).

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

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

15 (11) STATE.—The term “State”—

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

19 (B) includes any federally recognized In-
20 dian tribe that notifies the Secretary, not later
21 than 120 days after the date of the enactment
22 of this Act or not later than 120 days before
23 the start of any fiscal year during the 5-fiscal-
24 year period described in subsection (j), that the
25 tribe intends to develop a cyber resiliency plan

- 1 and agrees to forfeit any distribution under
- 2 subsection (f)(3).

○