

115TH CONGRESS
1ST SESSION

H. R. 1344

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

IN THE HOUSE OF REPRESENTATIVES

MARCH 2, 2017

Mr. KILMER (for himself and Mrs. COMSTOCK) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Transportation and Infrastructure, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

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”.

1 **SEC. 2. ESTABLISHMENT OF CYBER RESILIENCY GRANT**
2 **PROGRAM.**

3 (a) **ESTABLISHMENT.**—There is established the State
4 Cyber Resiliency Grant Program to assist State, local, and
5 tribal governments in preventing, preparing for, protecting
6 against, and responding to cyber threats, which shall be
7 administered by the Administrator of the Federal Emer-
8 gency Management Agency.

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

11 (c) **GRANTS AUTHORIZED FOR EACH STATE.**—Sub-
12 ject to the funds available under a funding allocation de-
13 termined under subsection (f) for a State, the Secretary
14 of Homeland Security may award to the State—

15 (1) up to 2 planning grants under subsection
16 (e) to develop or revise a cyber resiliency plan; and
17 (2) up to 2 implementation grants under sub-
18 section (f) to implement an active cyber resiliency
19 plan.

20 (d) **APPROVAL OF CYBER RESILIENCY PLANS.**—

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

1 (A) The plan incorporates, to the extent
2 practicable, any existing plans of such State to
3 protect against cybersecurity threats or
4 vulnerabilities.

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

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

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

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

1 tional Institute of Standards and Tech-
2 nology.

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

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

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

20 (vii) Accounting for and mitigating, to
21 the greatest degree possible, cybersecurity
22 threats or vulnerabilities related to critical
23 infrastructure or key resources, the deg-
24 radation of which may impact the perform-

1 ance of such functions within the State or
2 threaten public safety.

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

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

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

15 (II) as applicable, neighboring
16 countries.

17 (2) DURATION OF APPROVAL.—

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

22 (B) ANNUAL EXTENSION.—The Secretary
23 may annually extend such approval for a one-
24 year period, if the Secretary determines, after
25 considering the recommendations of the Review

1 Committee, that the plan continues to meet the
2 criteria described in paragraph (1) after the
3 State makes such revisions as the Secretary
4 may determine to be necessary.

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

11 (e) PLANNING GRANTS.—

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

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

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

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

1 Secretary for a determination under subsection
2 (d)(1).

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

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

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

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

17 (f) IMPLEMENTATION GRANTS.—

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

23 (A) A proposal, including a description and
24 timeline, of the activities to be funded by the

1 grant as described by a cyber resiliency plan of
2 the State approved under subsection (d).

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

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

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

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

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

1 (3) DISTRIBUTION TO LOCAL AND TRIBAL GOV-
2 ERNMENTS.—

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

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

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

21 (B) CONSULTATION.—In determining how
22 an implementation grant is distributed within a
23 State, the State shall consult with the local and
24 regional chief information officer, emergency

1 managers, and senior public safety officials of
2 the State.

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

6 (A) exclusively on a competitive basis; and

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

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

12 (g) USE OF GRANT FUNDS.—

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

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

20 (B) for any recreational or social purpose.

21 (2) APPROVED ACTIVITIES FOR IMPLEMENTA-
22 TION GRANTS.—A State or a government entity that
23 receives funds through a biennial implementation
24 grant may use such funds for one or more of the fol-

1 lowing activities, to the extent that such activities
2 are proposed under subsection (f)(1)(A):

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

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

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

14 (i) emergency management elements
15 of such State;

16 (ii) National Guard units, as appro-
17 priate;

18 (iii) entities associated with critical in-
19 frastructure or key resources;

20 (iv) information sharing and analysis
21 organizations;

22 (v) public safety answering points; or

23 (vi) nongovernmental organizations
24 engaged in cybersecurity research as a for-

1 mally designated information analysis and
2 sharing organization.

3 (D) Establishing programs, such as schol-
4 arships or apprenticeships, to provide financial
5 assistance to State residents who—

6 (i) pursue formal education, training,
7 and industry-recognized certifications for
8 careers in cybersecurity as identified by the
9 National Initiative for Cybersecurity Edu-
10 cation; and

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

13 (h) FUNDING ALLOCATIONS.—

14 (1) IN GENERAL.—From any amount appro-
15 priated for a fiscal year that is not reserved for use
16 by the Secretary in carrying out this section, the
17 Secretary shall allocate the entire amount among the
18 States (including the District of Columbia) eligible
19 for grants under this section taking into consider-
20 ation the factors specified in paragraph (2) and con-
21 sistent with the following:

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

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

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

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

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

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

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

24 (A) The considerations described in section
25 1809(h)(1) of the Homeland Security Act of

1 2002 (6 U.S.C. 579(h)(1)) with respect to the
2 State, and the degree of exposure of the State
3 and protected government entities within the
4 State to threats, vulnerabilities, or consequences
5 resulting from cybersecurity risks or incidents.

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

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

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

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

1 (i) REVIEW COMMITTEE FOR CYBER RESILIENCY
2 GRANTS.—

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

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

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

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

19 (B) review any plan or application for-
20 warded under paragraph (2);

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

1 (D) provide to the Secretary an evaluation
2 of any progress made by a State in imple-
3 menting an active cyber resiliency plan using a
4 prior biennial implementation grant; and

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

8 (4) MEMBERSHIP.—

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

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

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

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

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

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

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

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

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

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

1 of the Administrator, shall serve as the Vice
2 Chairperson of the Review Committee.

3 (5) STAFF AND EXPERTS.—The Review Com-
4 mittee may—

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

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

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

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

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

1 (8) TERMINATION.—The authority of the Re-
2 view Committee shall terminate on the day after the
3 end of the five-fiscal-year period described in sub-
4 section (c).

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

8 (k) DEFINITIONS.—In this section:

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

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

18 (3) CRITICAL INFRASTRUCTURE.—The term
19 “critical infrastructure” has the meaning given that
20 term in section 2 of the Homeland Security Act of
21 2002 (6 U.S.C. 101).

22 (4) CYBER RESILIENCY PLAN.—The term
23 “cyber resiliency plan” means, with respect to a
24 State, a plan that addresses the cybersecurity
25 threats or vulnerabilities faced by the State through

1 a statewide plan and decisionmaking process to re-
2 spond to cybersecurity risks or incidents.

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

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

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

15 (8) KEY RESOURCES.—The term “key re-
16 sources” has the meaning given that term in section
17 2 of the Homeland Security Act of 2002 (6 U.S.C.
18 101).

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

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

1 (11) STATE.—The term “State”—

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

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

○