

Union Calendar No. 31

117TH CONGRESS
1ST SESSION

H. R. 3138

[Report No. 117–48]

To amend the Homeland Security Act of 2002 to authorize a grant program relating to the cybersecurity of State and local governments, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MAY 12, 2021

Ms. CLARKE of New York (for herself, Mr. GARBARINO, Mr. KILMER, Mr. KATKO, Mr. RUPPERSBERGER, Mr. McCAUL, and Mr. THOMPSON of Mississippi) introduced the following bill; which was referred to the Committee on Homeland Security

JUNE 1, 2021

Additional sponsor: Ms. SLOTKIN

JUNE 1, 2021

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italic*]

[For text of introduced bill, see copy of bill as introduced on May 12, 2021]

A BILL

To amend the Homeland Security Act of 2002 to authorize a grant program relating to the cybersecurity of State and local governments, 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 and Local Cyberse-*
 5 *curity Improvement Act”.*

6 **SEC. 2. STATE AND LOCAL CYBERSECURITY GRANT PRO-**
 7 **GRAM.**

8 *(a) IN GENERAL.—Subtitle A of title XXII of the*
 9 *Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is*
 10 *amended by adding at the end the following new sections:*

11 **“SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT**
 12 **PROGRAM.**

13 *“(a) DEFINITIONS.—In this section:*

14 *“(1) CYBER THREAT INDICATOR.—The term*
 15 *‘cyber threat indicator’ has the meaning given the*
 16 *term in section 102 of the Cybersecurity Act of 2015*
 17 *(6 U.S.C. 1501).*

18 *“(2) CYBERSECURITY PLAN.—The term ‘Cyberse-*
 19 *curity Plan’ means a plan submitted by an eligible*
 20 *entity under subsection (e)(1).*

21 *“(3) ELIGIBLE ENTITY.—The term ‘eligible enti-*
 22 *ty’ means—*

23 *“(A) a State; or*

24 *“(B) an Indian tribe that, not later than*
 25 *120 days after the date of the enactment of this*

1 *section or not later than 120 days before the*
 2 *start of any fiscal year in which a grant under*
 3 *this section is awarded—*

4 *“(i) notifies the Secretary that the In-*
 5 *dian tribe intends to develop a Cybersecu-*
 6 *rity Plan; and*

7 *“(ii) agrees to forfeit any distribution*
 8 *under subsection (n)(2).*

9 *“(4) INCIDENT.—The term ‘incident’ has the*
 10 *meaning given the term in section 2209.*

11 *“(5) INDIAN TRIBE; TRIBAL ORGANIZATION.—The*
 12 *term ‘Indian tribe’ or ‘Tribal organization’ has the*
 13 *meaning given that term in section 4(e) of the of the*
 14 *Indian Self-Determination and Education Assistance*
 15 *Act (25 U.S.C. 5304(e)).*

16 *“(6) INFORMATION SHARING AND ANALYSIS OR-*
 17 *GANIZATION.—The term ‘information sharing and*
 18 *analysis organization’ has the meaning given the*
 19 *term in section 2222.*

20 *“(7) INFORMATION SYSTEM.—The term ‘informa-*
 21 *tion system’ has the meaning given the term in sec-*
 22 *tion 102 of the Cybersecurity Act of 2015 (6 U.S.C.*
 23 *1501).*

24 *“(8) ONLINE SERVICE.—The term ‘online service’*
 25 *means any internet-facing service, including a*

1 website, email, virtual private network, or custom ap-
2 plication.

3 “(9) *RANSOMWARE INCIDENT.*—The term
4 ‘ransomware incident’ means an incident that actu-
5 ally or imminently jeopardizes, without lawful au-
6 thority, the integrity, confidentiality, or availability
7 of information on an information system, or actually
8 or imminently jeopardizes, without lawful authority,
9 an information system for the purpose of coercing the
10 information system’s owner, operator, or another per-
11 son.

12 “(10) *STATE AND LOCAL CYBERSECURITY GRANT*
13 *PROGRAM.*—The term ‘State and Local Cybersecurity
14 Grant Program’ means the program established under
15 subsection (b).

16 “(11) *STATE AND LOCAL CYBERSECURITY RESIL-*
17 *IENCE COMMITTEE.*—The term ‘State and Local Cy-
18 bersecurity Resilience Committee’ means the com-
19 mittee established under subsection (o)(1).

20 “(b) *ESTABLISHMENT.*—

21 “(1) *IN GENERAL.*—The Secretary, acting
22 through the Director, shall establish a program, to be
23 known as the ‘the State and Local Cybersecurity
24 Grant Program’, to award grants to eligible entities
25 to address cybersecurity risks and cybersecurity

1 *threats to information systems of State, local, or Trib-*
2 *al organizations.*

3 “(2) *APPLICATION.—An eligible entity seeking a*
4 *grant under the State and Local Cybersecurity Grant*
5 *Program shall submit to the Secretary an application*
6 *at such time, in such manner, and containing such*
7 *information as the Secretary may require.*

8 “(c) *BASELINE REQUIREMENTS.—An eligible entity or*
9 *multistate group that receives a grant under this section*
10 *shall use the grant in compliance with—*

11 “(1)(A) *the Cybersecurity Plan of the eligible en-*
12 *tity or the Cybersecurity Plans of the eligible entities*
13 *that comprise the multistate group; and*

14 “(B) *the Homeland Security Strategy to Im-*
15 *prove the Cybersecurity of State, Local, Tribal, and*
16 *Territorial Governments developed under section*
17 *2210(e)(1); or*

18 “(2) *activities carried out under paragraphs (3),*
19 *(4), and (5) of subsection (h).*

20 “(d) *ADMINISTRATION.—The State and Local Cyberse-*
21 *curity Grant Program shall be administered in the same*
22 *office of the Department that administers grants made*
23 *under sections 2003 and 2004.*

24 “(e) *CYBERSECURITY PLANS.—*

1 “(1) *IN GENERAL.*—An eligible entity applying
2 for a grant under this section shall submit to the Sec-
3 retary a Cybersecurity Plan for approval.

4 “(2) *REQUIRED ELEMENTS.*—A Cybersecurity
5 Plan of an eligible entity shall—

6 “(A) incorporate, to the extent practicable,
7 any existing plans of the eligible entity to protect
8 against cybersecurity risks and cybersecurity
9 threats to information systems of State, local, or
10 Tribal organizations;

11 “(B) describe, to the extent practicable, how
12 the eligible entity will—

13 “(i) manage, monitor, and track infor-
14 mation systems, applications, and user ac-
15 counts owned or operated by or on behalf of
16 the eligible entity or by local or Tribal or-
17 ganizations within the jurisdiction of the el-
18 igible entity and the information technology
19 deployed on those information systems, in-
20 cluding legacy information systems and in-
21 formation technology that are no longer
22 supported by the manufacturer of the sys-
23 tems or technology;

24 “(ii) monitor, audit, and track activity
25 between information systems, applications,

1 *and user accounts owned or operated by or*
2 *on behalf of the eligible entity or by local or*
3 *Tribal organizations within the jurisdiction*
4 *of the eligible entity and between those in-*
5 *formation systems and information systems*
6 *not owned or operated by the eligible entity*
7 *or by local or Tribal organizations within*
8 *the jurisdiction of the eligible entity;*

9 “(iii) *enhance the preparation, re-*
10 *sponse, and resilience of information sys-*
11 *tems, applications, and user accounts owned*
12 *or operated by or on behalf of the eligible*
13 *entity or local or Tribal organizations*
14 *against cybersecurity risks and cybersecu-*
15 *rity threats;*

16 “(iv) *implement a process of contin-*
17 *uous cybersecurity vulnerability assessments*
18 *and threat mitigation practices prioritized*
19 *by degree of risk to address cybersecurity*
20 *risks and cybersecurity threats on informa-*
21 *tion systems of the eligible entity or local or*
22 *Tribal organizations;*

23 “(v) *ensure that State, local, and Trib-*
24 *al organizations that own or operate infor-*

1 *mation systems that are located within the*
2 *jurisdiction of the eligible entity—*

3 *“(I) adopt best practices and*
4 *methodologies to enhance cybersecurity,*
5 *such as the practices set forth in the*
6 *cybersecurity framework developed by,*
7 *and the cyber supply chain risk man-*
8 *agement best practices identified by,*
9 *the National Institute of Standards*
10 *and Technology; and*

11 *“(II) utilize knowledge bases of*
12 *adversary tools and tactics to assess*
13 *risk;*

14 *“(vi) promote the delivery of safe, rec-*
15 *ognizable, and trustworthy online services*
16 *by State, local, and Tribal organizations,*
17 *including through the use of the .gov inter-*
18 *net domain;*

19 *“(vii) ensure continuity of operations*
20 *of the eligible entity and local, and Tribal*
21 *organizations in the event of a cybersecurity*
22 *incident (including a ransomware inci-*
23 *dent), including by conducting exercises to*
24 *practice responding to such an incident;*

1 “(viii) use the National Initiative for
2 Cybersecurity Education Cybersecurity
3 Workforce Framework developed by the Na-
4 tional Institute of Standards and Tech-
5 nology to identify and mitigate any gaps in
6 the cybersecurity workforces of State, local,
7 or Tribal organizations, enhance recruit-
8 ment and retention efforts for such
9 workforces, and bolster the knowledge, skills,
10 and abilities of State, local, and Tribal or-
11 ganization personnel to address cybersecu-
12 rity risks and cybersecurity threats, such as
13 through cybersecurity hygiene training;

14 “(ix) ensure continuity of communica-
15 tions and data networks within the jurisdic-
16 tion of the eligible entity between the eligible
17 entity and local and Tribal organizations
18 that own or operate information systems
19 within the jurisdiction of the eligible entity
20 in the event of an incident involving such
21 communications or data networks within
22 the jurisdiction of the eligible entity;

23 “(x) assess and mitigate, to the greatest
24 degree possible, cybersecurity risks and cy-
25 bersecurity threats related to critical infra-

1 *structure and key resources, the degradation*
2 *of which may impact the performance of in-*
3 *formation systems within the jurisdiction of*
4 *the eligible entity;*

5 “(xi) *enhance capabilities to share*
6 *cyber threat indicators and related informa-*
7 *tion between the eligible entity and local*
8 *and Tribal organizations that own or oper-*
9 *ate information systems within the jurisdic-*
10 *tion of the eligible entity, including by ex-*
11 *panding existing information sharing*
12 *agreements with the Department;*

13 “(xii) *enhance the capability of the eli-*
14 *gible entity to share cyber threat indictors*
15 *and related information with the Depart-*
16 *ment;*

17 “(xiii) *leverage cybersecurity services*
18 *offered by the Department;*

19 “(xiv) *develop and coordinate strate-*
20 *gies to address cybersecurity risks and cy-*
21 *bersecurity threats to information systems*
22 *of the eligible entity in consultation with—*

23 “(I) *local and Tribal organiza-*
24 *tions within the jurisdiction of the eli-*
25 *gible entity; and*

1 “(II) as applicable—

2 “(aa) States that neighbor
3 the jurisdiction of the eligible en-
4 tity or, as appropriate, members
5 of an information sharing and
6 analysis organization; and

7 “(bb) countries that neighbor
8 the jurisdiction of the eligible en-
9 tity; and

10 “(xv) implement an information tech-
11 nology and operational technology mod-
12 ernization cybersecurity review process that
13 ensures alignment between information
14 technology and operational technology cy-
15 bersecurity objectives;

16 “(C) describe, to the extent practicable, the
17 individual responsibilities of the eligible entity
18 and local and Tribal organizations within the
19 jurisdiction of the eligible entity in imple-
20 menting the plan;

21 “(D) outline, to the extent practicable, the
22 necessary resources and a timeline for imple-
23 menting the plan; and

1 “(E) describe how the eligible entity will
2 measure progress towards implementing the
3 plan.

4 “(3) *DISCRETIONARY ELEMENTS.*—A Cybersecu-
5 rity Plan of an eligible entity may include a descrip-
6 tion of—

7 “(A) cooperative programs developed by
8 groups of local and Tribal organizations within
9 the jurisdiction of the eligible entity to address
10 cybersecurity risks and cybersecurity threats;
11 and

12 “(B) programs provided by the eligible enti-
13 ty to support local and Tribal organizations and
14 owners and operators of critical infrastructure to
15 address cybersecurity risks and cybersecurity
16 threats.

17 “(4) *MANAGEMENT OF FUNDS.*—An eligible enti-
18 ty applying for a grant under this section shall agree
19 to designate the Chief Information Officer, the Chief
20 Information Security Officer, or an equivalent official
21 of the eligible entity as the primary official for the
22 management and allocation of funds awarded under
23 this section.

24 “(f) *MULTISTATE GRANTS.*—

1 “(1) *IN GENERAL.*—*The Secretary, acting*
 2 *through the Director, may award grants under this*
 3 *section to a group of two or more eligible entities to*
 4 *support multistate efforts to address cybersecurity*
 5 *risks and cybersecurity threats to information systems*
 6 *within the jurisdictions of the eligible entities.*

7 “(2) *SATISFACTION OF OTHER REQUIRE-*
 8 *MENTS.*—*In order to be eligible for a multistate grant*
 9 *under this subsection, each eligible entity that com-*
 10 *prises a multistate group shall submit to the Sec-*
 11 *retary—*

12 “(A) *a Cybersecurity Plan for approval in*
 13 *accordance with subsection (i); and*

14 “(B) *a plan for establishing a cybersecurity*
 15 *planning committee under subsection (g).*

16 “(3) *APPLICATION.*—

17 “(A) *IN GENERAL.*—*A multistate group ap-*
 18 *plying for a multistate grant under paragraph*
 19 *(1) shall submit to the Secretary an application*
 20 *at such time, in such manner, and containing*
 21 *such information as the Secretary may require.*

22 “(B) *MULTISTATE PROJECT DESCRIP-*
 23 *TION.*—*An application of a multistate group*
 24 *under subparagraph (A) shall include a plan de-*
 25 *scribing—*

1 “(i) the division of responsibilities
2 among the eligible entities that comprise the
3 multistate group for administering the
4 grant for which application is being made;

5 “(ii) the distribution of funding from
6 such a grant among the eligible entities that
7 comprise the multistate group; and

8 “(iii) how the eligible entities that
9 comprise the multistate group will work to-
10 gether to implement the Cybersecurity Plan
11 of each of those eligible entities.

12 “(g) *PLANNING COMMITTEES.*—

13 “(1) *IN GENERAL.*—An eligible entity that re-
14 ceives a grant under this section shall establish a cy-
15 bersecurity planning committee to—

16 “(A) assist in the development, implementa-
17 tion, and revision of the Cybersecurity Plan of
18 the eligible entity;

19 “(B) approve the Cybersecurity Plan of the
20 eligible entity; and

21 “(C) assist in the determination of effective
22 funding priorities for a grant under this section
23 in accordance with subsection (h).

24 “(2) *COMPOSITION.*—A committee of an eligible
25 entity established under paragraph (1) shall—

1 “(A) be comprised of representatives from
 2 the eligible entity and counties, cities, towns,
 3 Tribes, and public educational and health insti-
 4 tutions within the jurisdiction of the eligible en-
 5 tity; and

6 “(B) include, as appropriate, representa-
 7 tives of rural, suburban, and high-population ju-
 8 risdictions.

9 “(3) CYBERSECURITY EXPERTISE.—Not less than
 10 $\frac{1}{2}$ of the representatives of a committee established
 11 under paragraph (1) shall have professional experi-
 12 ence relating to cybersecurity or information tech-
 13 nology.

14 “(4) RULE OF CONSTRUCTION REGARDING EXIST-
 15 ING PLANNING COMMITTEES.—Nothing in this sub-
 16 section may be construed to require an eligible entity
 17 to establish a cybersecurity planning committee if the
 18 eligible entity has established and uses a multijuris-
 19 dictional planning committee or commission that
 20 meets, or may be leveraged to meet, the requirements
 21 of this subsection.

22 “(h) USE OF FUNDS.—An eligible entity that receives
 23 a grant under this section shall use the grant to—

24 “(1) implement the Cybersecurity Plan of the eli-
 25 gible entity;

1 “(2) *develop or revise the Cybersecurity Plan of*
2 *the eligible entity; or*

3 “(3) *assist with activities that address imminent*
4 *cybersecurity risks or cybersecurity threats to the in-*
5 *formation systems of the eligible entity or a local or*
6 *Tribal organization within the jurisdiction of the eli-*
7 *gible entity.*

8 “(i) *APPROVAL OF PLANS.—*

9 “(1) *APPROVAL AS CONDITION OF GRANT.—Be-*
10 *fore an eligible entity may receive a grant under this*
11 *section, the Secretary, acting through the Director,*
12 *shall review the Cybersecurity Plan, or any revisions*
13 *thereto, of the eligible entity and approve such plan,*
14 *or revised plan, if it satisfies the requirements speci-*
15 *fied in paragraph (2).*

16 “(2) *PLAN REQUIREMENTS.—In approving a Cy-*
17 *bersecurity Plan of an eligible entity under this sub-*
18 *section, the Director shall ensure that the Cybersecu-*
19 *rity Plan—*

20 “(A) *satisfies the requirements of subsection*
21 *(e)(2);*

22 “(B) *upon the issuance of the Homeland Se-*
23 *curity Strategy to Improve the Cybersecurity of*
24 *State, Local, Tribal, and Territorial Govern-*
25 *ments authorized pursuant to section 2210(e),*

1 *complies, as appropriate, with the goals and ob-*
2 *jectives of the strategy; and*

3 *“(C) has been approved by the cybersecurity*
4 *planning committee of the eligible entity estab-*
5 *lished under subsection (g).*

6 *“(3) APPROVAL OF REVISIONS.—The Secretary,*
7 *acting through the Director, may approve revisions to*
8 *a Cybersecurity Plan as the Director determines ap-*
9 *propriate.*

10 *“(4) EXCEPTION.—Notwithstanding subsection*
11 *(e) and paragraph (1) of this subsection, the Sec-*
12 *retary may award a grant under this section to an*
13 *eligible entity that does not submit a Cybersecurity*
14 *Plan to the Secretary if—*

15 *“(A) the eligible entity certifies to the Sec-*
16 *retary that—*

17 *“(i) the activities that will be sup-*
18 *ported by the grant are integral to the de-*
19 *velopment of the Cybersecurity Plan of the*
20 *eligible entity; and*

21 *“(ii) the eligible entity will submit by*
22 *September 30, 2023, to the Secretary a Cy-*
23 *bersecurity Plan for review, and if appro-*
24 *priate, approval; or*

1 “(B) the eligible entity certifies to the Sec-
 2 retary, and the Director confirms, that the eligi-
 3 ble entity will use funds from the grant to assist
 4 with the activities described in subsection (h)(3).

5 “(j) *LIMITATIONS ON USES OF FUNDS.*—

6 “(1) *IN GENERAL.*—An eligible entity that re-
 7 ceives a grant under this section may not use the
 8 grant—

9 “(A) to supplant State, local, or Tribal
 10 funds;

11 “(B) for any recipient cost-sharing con-
 12 tribution;

13 “(C) to pay a demand for ransom in an at-
 14 tempt to—

15 “(i) regain access to information or an
 16 information system of the eligible entity or
 17 of a local or Tribal organization within the
 18 jurisdiction of the eligible entity; or

19 “(ii) prevent the disclosure of informa-
 20 tion that has been removed without author-
 21 ization from an information system of the
 22 eligible entity or of a local or Tribal organi-
 23 zation within the jurisdiction of the eligible
 24 entity;

25 “(D) for recreational or social purposes; or

1 “(E) for any purpose that does not address
2 cybersecurity risks or cybersecurity threats on
3 information systems of the eligible entity or of a
4 local or Tribal organization within the jurisdic-
5 tion of the eligible entity.

6 “(2) *PENALTIES.*—In addition to any other rem-
7 edy available, the Secretary may take such actions as
8 are necessary to ensure that a recipient of a grant
9 under this section uses the grant for the purposes for
10 which the grant is awarded.

11 “(3) *RULE OF CONSTRUCTION.*—Nothing in
12 paragraph (1) may be construed to prohibit the use
13 of grant funds provided to a State, local, or Tribal
14 organization for otherwise permissible uses under this
15 section on the basis that a State, local, or Tribal or-
16 ganization has previously used State, local, or Tribal
17 funds to support the same or similar uses.

18 “(k) *OPPORTUNITY TO AMEND APPLICATIONS.*—In
19 considering applications for grants under this section, the
20 Secretary shall provide applicants with a reasonable oppor-
21 tunity to correct defects, if any, in such applications before
22 making final awards.

23 “(l) *APPORTIONMENT.*—For fiscal year 2022 and each
24 fiscal year thereafter, the Secretary shall apportion

1 *amounts appropriated to carry out this section among*
2 *States as follows:*

3 “(1) *BASELINE AMOUNT.—The Secretary shall*
4 *first apportion 0.25 percent of such amounts to each*
5 *of American Samoa, the Commonwealth of the North-*
6 *ern Mariana Islands, Guam, the U.S. Virgin Islands,*
7 *and 0.75 percent of such amounts to each of the re-*
8 *maining States.*

9 “(2) *REMAINDER.—The Secretary shall appor-*
10 *tion the remainder of such amounts in the ratio*
11 *that—*

12 “(A) *the population of each eligible entity,*
13 *bears to*

14 “(B) *the population of all eligible entities.*

15 “(3) *MINIMUM ALLOCATION TO INDIAN TRIBES.—*

16 “(A) *IN GENERAL.—In apportioning*
17 *amounts under this section, the Secretary shall*
18 *ensure that, for each fiscal year, directly eligible*
19 *Tribes collectively receive, from amounts appro-*
20 *priated under the State and Local Cybersecurity*
21 *Grant Program, not less than an amount equal*
22 *to three percent of the total amount appropriated*
23 *for grants under this section.*

24 “(B) *ALLOCATION.—Of the amount reserved*
25 *under subparagraph (A), funds shall be allocated*

1 *in a manner determined by the Secretary in con-*
 2 *sultation with Indian tribes.*

3 “(C) *EXCEPTION.—This paragraph shall*
 4 *not apply in any fiscal year in which the Sec-*
 5 *retary—*

6 *“(i) receives fewer than five applica-*
 7 *tions from Indian tribes; or*

8 *“(ii) does not approve at least two ap-*
 9 *plication from Indian tribes.*

10 “(m) *FEDERAL SHARE.—*

11 *“(1) IN GENERAL.—The Federal share of the cost*
 12 *of an activity carried out using funds made available*
 13 *with a grant under this section may not exceed—*

14 *“(A) in the case of a grant to an eligible en-*
 15 *tity—*

16 *“(i) for fiscal year 2022, 90 percent;*

17 *“(ii) for fiscal year 2023, 80 percent;*

18 *“(iii) for fiscal year 2024, 70 percent;*

19 *“(iv) for fiscal year 2025, 60 percent;*

20 *and*

21 *“(v) for fiscal year 2026 and each sub-*
 22 *sequent fiscal year, 50 percent; and*

23 *“(B) in the case of a grant to a multistate*
 24 *group—*

25 *“(i) for fiscal year 2022, 95 percent;*

1 “(ii) for fiscal year 2023, 85 percent;

2 “(iii) for fiscal year 2024, 75 percent;

3 “(iv) for fiscal year 2025, 65 percent;

4 and

5 “(v) for fiscal year 2026 and each sub-
6 sequent fiscal year, 55 percent.

7 “(2) *WAIVER.*—*The Secretary may waive or*
8 *modify the requirements of paragraph (1) for an In-*
9 *Indian tribe if the Secretary determines such a waiver*
10 *is in the public interest.*

11 “(n) *RESPONSIBILITIES OF GRANTEES.*—

12 “(1) *CERTIFICATION.*—*Each eligible entity or*
13 *multistate group that receives a grant under this sec-*
14 *tion shall certify to the Secretary that the grant will*
15 *be used—*

16 “(A) *for the purpose for which the grant is*
17 *awarded; and*

18 “(B) *in compliance with, as the case may*
19 *be—*

20 “(i) *the Cybersecurity Plan of the eligi-*
21 *ble entity;*

22 “(ii) *the Cybersecurity Plans of the eli-*
23 *gible entities that comprise the multistate*
24 *group; or*

1 “(iii) a purpose approved by the Sec-
2 retary under subsection (h) or pursuant to
3 an exception under subsection (i).

4 “(2) AVAILABILITY OF FUNDS TO LOCAL AND
5 TRIBAL ORGANIZATIONS.—Not later than 45 days
6 after the date on which an eligible entity or
7 multistate group receives a grant under this section,
8 the eligible entity or multistate group shall, without
9 imposing unreasonable or unduly burdensome re-
10 quirements as a condition of receipt, obligate or other-
11 wise make available to local and Tribal organizations
12 within the jurisdiction of the eligible entity or the eli-
13 gible entities that comprise the multistate group, and
14 as applicable, consistent with the Cybersecurity Plan
15 of the eligible entity or the Cybersecurity Plans of the
16 eligible entities that comprise the multistate group—

17 “(A) not less than 80 percent of funds avail-
18 able under the grant;

19 “(B) with the consent of the local and Trib-
20 al organizations, items, services, capabilities, or
21 activities having a value of not less than 80 per-
22 cent of the amount of the grant; or

23 “(C) with the consent of the local and Trib-
24 al organizations, grant funds combined with
25 other items, services, capabilities, or activities

1 *having the total value of not less than 80 percent*
2 *of the amount of the grant.*

3 “(3) *CERTIFICATIONS REGARDING DISTRIBUTION*
4 *OF GRANT FUNDS TO LOCAL AND TRIBAL ORGANIZA-*
5 *TIONS.—An eligible entity or multistate group shall*
6 *certify to the Secretary that the eligible entity or*
7 *multistate group has made the distribution to local,*
8 *Tribal, and territorial governments required under*
9 *paragraph (2).*

10 “(4) *EXTENSION OF PERIOD.—*

11 “(A) *IN GENERAL.—An eligible entity or*
12 *multistate group may request in writing that the*
13 *Secretary extend the period of time specified in*
14 *paragraph (2) for an additional period of time.*

15 “(B) *APPROVAL.—The Secretary may ap-*
16 *prove a request for an extension under subpara-*
17 *graph (A) if the Secretary determines the exten-*
18 *sion is necessary to ensure that the obligation*
19 *and expenditure of grant funds align with the*
20 *purpose of the State and Local Cybersecurity*
21 *Grant Program.*

22 “(5) *EXCEPTION.—Paragraph (2) shall not*
23 *apply to the District of Columbia, the Commonwealth*
24 *of Puerto Rico, American Samoa, the Commonwealth*

1 *of the Northern Mariana Islands, Guam, the Virgin*
2 *Islands, or an Indian tribe.*

3 “(6) *DIRECT FUNDING.*—*If an eligible entity*
4 *does not make a distribution to a local or Tribal or-*
5 *ganization required in accordance with paragraph*
6 *(2), the local or Tribal organization may petition the*
7 *Secretary to request that grant funds be provided di-*
8 *rectly to the local or Tribal organization.*

9 “(7) *PENALTIES.*—*In addition to other remedies*
10 *available to the Secretary, the Secretary may termi-*
11 *nate or reduce the amount of a grant awarded under*
12 *this section to an eligible entity or distribute grant*
13 *funds previously awarded to such eligible entity di-*
14 *rectly to the appropriate local or Tribal organization*
15 *as a replacement grant in an amount the Secretary*
16 *determines appropriate if such eligible entity violates*
17 *a requirement of this subsection.*

18 “(o) *ADVISORY COMMITTEE.*—

19 “(1) *ESTABLISHMENT.*—*Not later than 120 days*
20 *after the date of enactment of this section, the Direc-*
21 *tor shall establish a State and Local Cybersecurity*
22 *Resilience Committee to provide State, local, and*
23 *Tribal stakeholder expertise, situational awareness,*
24 *and recommendations to the Director, as appropriate,*
25 *regarding how to—*

1 “(A) address cybersecurity risks and cyber-
2 security threats to information systems of State,
3 local, or Tribal organizations; and

4 “(B) improve the ability of State, local, and
5 Tribal organizations to prevent, protect against,
6 respond to, mitigate, and recover from such cy-
7 bersecurity risks and cybersecurity threats.

8 “(2) DUTIES.—The committee established under
9 paragraph (1) shall—

10 “(A) submit to the Director recommenda-
11 tions that may inform guidance for applicants
12 for grants under this section;

13 “(B) upon the request of the Director, pro-
14 vide to the Director technical assistance to in-
15 form the review of Cybersecurity Plans submitted
16 by applicants for grants under this section, and,
17 as appropriate, submit to the Director rec-
18 ommendations to improve those plans prior to
19 the approval of the plans under subsection (i);

20 “(C) advise and provide to the Director
21 input regarding the Homeland Security Strategy
22 to Improve Cybersecurity for State, Local, Trib-
23 al, and Territorial Governments required under
24 section 2210;

1 “(D) upon the request of the Director, pro-
2 vide to the Director recommendations, as appro-
3 priate, regarding how to—

4 “(i) address cybersecurity risks and cy-
5 bersecurity threats on information systems
6 of State, local, or Tribal organizations; and

7 “(ii) improve the cybersecurity resil-
8 ience of State, local, or Tribal organiza-
9 tions; and

10 “(E) regularly coordinate with the State,
11 Local, Tribal and Territorial Government Co-
12 ordinating Council, within the Critical Infra-
13 structure Partnership Advisory Council, estab-
14 lished under section 871.

15 “(3) MEMBERSHIP.—

16 “(A) NUMBER AND APPOINTMENT.—The
17 State and Local Cybersecurity Resilience Com-
18 mittee established pursuant to paragraph (1)
19 shall be composed of 15 members appointed by
20 the Director, as follows:

21 “(i) Two individuals recommended to
22 the Director by the National Governors As-
23 sociation.

1 “(ii) *Two individuals recommended to*
2 *the Director by the National Association of*
3 *State Chief Information Officers.*

4 “(iii) *One individual recommended to*
5 *the Director by the National Guard Bureau.*

6 “(iv) *Two individuals recommended to*
7 *the Director by the National Association of*
8 *Counties.*

9 “(v) *One individual recommended to*
10 *the Director by the National League of Cit-*
11 *ies.*

12 “(vi) *One individual recommended to*
13 *the Director by the United States Con-*
14 *ference of Mayors.*

15 “(vii) *One individual recommended to*
16 *the Director by the Multi-State Information*
17 *Sharing and Analysis Center.*

18 “(viii) *One individual recommended to*
19 *the Director by the National Congress of*
20 *American Indians.*

21 “(viii) *Four individuals who have edu-*
22 *cational and professional experience relat-*
23 *ing to cybersecurity work or cybersecurity*
24 *policy.*

25 “(B) *TERMS.—*

1 “(i) *IN GENERAL.*—Subject to clause
2 (ii), each member of the State and Local
3 Cybersecurity Resilience Committee shall be
4 appointed for a term of two years.

5 “(ii) *REQUIREMENT.*—At least two
6 members of the State and Local Cybersecu-
7 rity Resilience Committee shall also be
8 members of the State, Local, Tribal and
9 Territorial Government Coordinating Coun-
10 cil, within the Critical Infrastructure Part-
11 nership Advisory Council, established under
12 section 871.

13 “(iii) *EXCEPTION.*—A term of a mem-
14 ber of the State and Local Cybersecurity
15 Resilience Committee shall be three years if
16 the member is appointed initially to the
17 Committee upon the establishment of the
18 Committee.

19 “(iv) *TERM REMAINDERS.*—Any mem-
20 ber of the State and Local Cybersecurity
21 Resilience Committee appointed to fill a va-
22 cancy occurring before the expiration of the
23 term for which the member’s predecessor
24 was appointed shall be appointed only for
25 the remainder of such term. A member may

1 *serve after the expiration of such member's*
2 *term until a successor has taken office.*

3 “(v) *VACANCIES.*—*A vacancy in the*
4 *State and Local Cybersecurity Resilience*
5 *Committee shall be filled in the manner in*
6 *which the original appointment was made.*

7 “(C) *PAY.*—*Members of the State and Local*
8 *Cybersecurity Resilience Committee shall serve*
9 *without pay.*

10 “(4) *CHAIRPERSON; VICE CHAIRPERSON.*—*The*
11 *members of the State and Local Cybersecurity Resil-*
12 *ience Committee shall select a chairperson and vice*
13 *chairperson from among members of the committee.*

14 “(5) *PERMANENT AUTHORITY.*—*Notwithstanding*
15 *section 14 of the Federal Advisory Committee Act (5*
16 *U.S.C. App.), the State and Local Cybersecurity Re-*
17 *silience Committee shall be a permanent authority.*

18 “(p) *REPORTS.*—

19 “(1) *ANNUAL REPORTS BY GRANT RECIPIENTS.*—

20 “(A) *IN GENERAL.*—*Not later than one year*
21 *after an eligible entity or multistate group re-*
22 *ceives funds under this section, the eligible entity*
23 *or multistate group shall submit to the Secretary*
24 *a report on the progress of the eligible entity or*
25 *multistate group in implementing the Cybersecu-*

1 *urity Plan of the eligible entity or Cybersecurity*
 2 *Plans of the eligible entities that comprise the*
 3 *multistate group, as the case may be.*

4 “(B) *ABSENCE OF PLAN.*—Not later than
 5 *180 days after an eligible entity that does not*
 6 *have a Cybersecurity Plan receives funds under*
 7 *this section for developing its Cybersecurity*
 8 *Plan, the eligible entity shall submit to the Sec-*
 9 *retary a report describing how the eligible entity*
 10 *obligated and expended grant funds during the*
 11 *fiscal year to—*

12 “(i) *so develop such a Cybersecurity*
 13 *Plan; or*

14 “(ii) *assist with the activities described*
 15 *in subsection (h)(3).*

16 “(2) *ANNUAL REPORTS TO CONGRESS.*—Not less
 17 *frequently than once per year, the Secretary, acting*
 18 *through the Director, shall submit to Congress a re-*
 19 *port on the use of grants awarded under this section*
 20 *and any progress made toward the following:*

21 “(A) *Achieving the objectives set forth in the*
 22 *Homeland Security Strategy to Improve the Cy-*
 23 *bersecurity of State, Local, Tribal, and Terri-*
 24 *torial Governments, upon the date on which the*
 25 *strategy is issued under section 2210.*

1 “(B) *Developing, implementing, or revising*
 2 *Cybersecurity Plans.*

3 “(C) *Reducing cybersecurity risks and cy-*
 4 *bersecurity threats to information systems, ap-*
 5 *plications, and user accounts owned or operated*
 6 *by or on behalf of State, local, and Tribal orga-*
 7 *nizations as a result of the award of such grants.*

8 “(q) *AUTHORIZATION OF APPROPRIATIONS.—There*
 9 *are authorized to be appropriated for grants under this sec-*
 10 *tion—*

11 “(1) *for each of fiscal years 2022 through 2026,*
 12 *\$500,000,000; and*

13 “(2) *for each subsequent fiscal year, such sums*
 14 *as may be necessary.*

15 **“SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOP-**
 16 **MENT FOR STATE, LOCAL, TRIBAL, AND TER-**
 17 **RITORIAL GOVERNMENT OFFICIALS.**

18 *“The Secretary, acting through the Director, shall de-*
 19 *velop, regularly update, and maintain a resource guide for*
 20 *use by State, local, Tribal, and territorial government offi-*
 21 *cials, including law enforcement officers, to help such offi-*
 22 *cials identify, prepare for, detect, protect against, respond*
 23 *to, and recover from cybersecurity risks (as such term is*
 24 *defined in section 2209), cybersecurity threats, and inci-*
 25 *dents (as such term is defined in section 2209).”.*

1 (b) *CLERICAL AMENDMENT.*—*The table of contents in*
 2 *section 1(b) of the Homeland Security Act of 2002, as*
 3 *amended by section 4, is further amended by inserting after*
 4 *the item relating to section 2220 the following new items:*

“Sec. 2220A. *State and Local Cybersecurity Grant Program.*

“Sec. 2220B. *Cybersecurity resource guide development for State, local, Tribal, and territorial government officials.*”.

5 **SEC. 3. STRATEGY.**

6 (a) *HOMELAND SECURITY STRATEGY TO IMPROVE THE*
 7 *CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TERRI-*
 8 *TORIAL GOVERNMENTS.*—*Section 2210 of the Homeland Se-*
 9 *curity Act of 2002 (6 U.S.C. 660) is amended by adding*
 10 *at the end the following new subsection:*

11 “(e) *HOMELAND SECURITY STRATEGY TO IMPROVE*
 12 *THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TER-*
 13 *RITORIAL GOVERNMENTS.*—

14 “(1) *IN GENERAL.*—

15 “(A) *REQUIREMENT.*—*Not later than one*
 16 *year after the date of the enactment of this sub-*
 17 *section, the Secretary, acting through the Direc-*
 18 *tor, shall, in coordination with the heads of ap-*
 19 *propriate Federal agencies, State, local, Tribal,*
 20 *and territorial governments, the State and Local*
 21 *Cybersecurity Resilience Committee established*
 22 *under section 2220A, and other stakeholders, as*
 23 *appropriate, develop and make publicly avail-*
 24 *able a Homeland Security Strategy to Improve*

1 *the Cybersecurity of State, Local, Tribal, and*
2 *Territorial Governments.*

3 “(B) *RECOMMENDATIONS AND REQUIRE-*
4 *MENTS.—The strategy required under subpara-*
5 *graph (A) shall—*

6 “(i) *provide recommendations relating*
7 *to the ways in which the Federal Govern-*
8 *ment should support and promote the abil-*
9 *ity of State, local, Tribal, and territorial*
10 *governments to identify, mitigate against,*
11 *protect against, detect, respond to, and re-*
12 *cover from cybersecurity risks (as such term*
13 *is defined in section 2209), cybersecurity*
14 *threats, and incidents (as such term is de-*
15 *finied in section 2209); and*

16 “(ii) *establish baseline requirements for*
17 *cybersecurity plans under this section and*
18 *principles with which such plans shall*
19 *align.*

20 “(2) *CONTENTS.—The strategy required under*
21 *paragraph (1) shall—*

22 “(A) *identify capability gaps in the ability*
23 *of State, local, Tribal, and territorial govern-*
24 *ments to identify, protect against, detect, respond*
25 *to, and recover from cybersecurity risks, cyberse-*

1 *curity threats, incidents, and ransomware inci-*
2 *dents;*

3 *“(B) identify Federal resources and capa-*
4 *bilities that are available or could be made*
5 *available to State, local, Tribal, and territorial*
6 *governments to help those governments identify,*
7 *protect against, detect, respond to, and recover*
8 *from cybersecurity risks, cybersecurity threats,*
9 *incidents, and ransomware incidents;*

10 *“(C) identify and assess the limitations of*
11 *Federal resources and capabilities available to*
12 *State, local, Tribal, and territorial governments*
13 *to help those governments identify, protect*
14 *against, detect, respond to, and recover from cy-*
15 *bersecurity risks, cybersecurity threats, incidents,*
16 *and ransomware incidents and make rec-*
17 *ommendations to address such limitations;*

18 *“(D) identify opportunities to improve the*
19 *coordination of the Agency with Federal and*
20 *non-Federal entities, such as the Multi-State In-*
21 *formation Sharing and Analysis Center, to im-*
22 *prove—*

23 *“(i) incident exercises, information*
24 *sharing and incident notification proce-*
25 *dures;*

1 “(ii) the ability for State, local, Tribal,
2 and territorial governments to voluntarily
3 adapt and implement guidance in Federal
4 binding operational directives; and

5 “(iii) opportunities to leverage Federal
6 schedules for cybersecurity investments
7 under section 502 of title 40, United States
8 Code;

9 “(E) recommend new initiatives the Federal
10 Government should undertake to improve the
11 ability of State, local, Tribal, and territorial
12 governments to identify, protect against, detect,
13 respond to, and recover from cybersecurity risks,
14 cybersecurity threats, incidents, and ransomware
15 incidents;

16 “(F) set short-term and long-term goals that
17 will improve the ability of State, local, Tribal,
18 and territorial governments to identify, protect
19 against, detect, respond to, and recover from cy-
20 bersecurity risks, cybersecurity threats, incidents,
21 and ransomware incidents; and

22 “(G) set dates, including interim bench-
23 marks, as appropriate for State, local, Tribal,
24 and territorial governments to establish baseline
25 capabilities to identify, protect against, detect,

1 respond to, and recover from cybersecurity risks,
2 cybersecurity threats, incidents, and ransomware
3 incidents.

4 “(3) *CONSIDERATIONS.*—In developing the strat-
5 egy required under paragraph (1), the Director, in co-
6 ordination with the heads of appropriate Federal
7 agencies, State, local, Tribal, and territorial govern-
8 ments, the State and Local Cybersecurity Resilience
9 Committee established under section 2220A, and other
10 stakeholders, as appropriate, shall consider—

11 “(A) lessons learned from incidents that
12 have affected State, local, Tribal, and territorial
13 governments, and exercises with Federal and
14 non-Federal entities;

15 “(B) the impact of incidents that have af-
16 fected State, local, Tribal, and territorial govern-
17 ments, including the resulting costs to such gov-
18 ernments;

19 “(C) the information related to the interest
20 and ability of state and non-state threat actors
21 to compromise information systems (as such
22 term is defined in section 102 of the Cybersecu-
23 rity Act of 2015 (6 U.S.C. 1501)) owned or oper-
24 ated by State, local, Tribal, and territorial gov-
25 ernments;

1 “(D) *emerging cybersecurity risks and cy-*
 2 *bersecurity threats to State, local, Tribal, and*
 3 *territorial governments resulting from the de-*
 4 *ployment of new technologies; and*

5 “(E) *recommendations made by the State*
 6 *and Local Cybersecurity Resilience Committee*
 7 *established under section 2220A.*

8 “(4) *EXEMPTION.—Chapter 35 of title 44,*
 9 *United States Code (commonly known as the ‘Paper-*
 10 *work Reduction Act’), shall not apply to any action*
 11 *to implement this subsection.”.*

12 ***(b) RESPONSIBILITIES OF THE DIRECTOR OF THE CY-***
 13 ***BERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—***
 14 *Section 2202 of the Homeland Security Act of 2002 (6*
 15 *U.S.C. 652) is amended—*

16 *(1) by redesignating subsections (d) through (i)*
 17 *as subsections (e) through (j), respectively; and*

18 *(2) by inserting after subsection (c) the following*
 19 *new subsection:*

20 “(d) *ADDITIONAL RESPONSIBILITIES.—In addition to*
 21 *the responsibilities under subsection (c), the Director*
 22 *shall—*

23 *“(1) develop program guidance, in consultation*
 24 *with the State and Local Government Cybersecurity*
 25 *Resilience Committee established under section 2220A,*

1 *for the State and Local Cybersecurity Grant Program*
2 *under such section or any other homeland security as-*
3 *sistance administered by the Department to improve*
4 *cybersecurity;*

5 “(2) review, in consultation with the State and
6 *Local Cybersecurity Resilience Committee, all cyberse-*
7 *curity plans of State, local, Tribal, and territorial*
8 *governments developed pursuant to any homeland se-*
9 *curity assistance administered by the Department to*
10 *improve cybersecurity;*

11 “(3) provide expertise and technical assistance to
12 *State, local, Tribal, and territorial government offi-*
13 *cials with respect to cybersecurity; and*

14 “(4) provide education, training, and capacity
15 *development to enhance the security and resilience of*
16 *cybersecurity and infrastructure security.”.*

17 (c) *FEASIBILITY STUDY.*—Not later than 270 days
18 *after the date of the enactment of this Act, the Director of*
19 *the Cybersecurity and Infrastructure Security of the De-*
20 *partment of Homeland Security shall conduct a study to*
21 *assess the feasibility of implementing a short-term rota-*
22 *tional program for the detail to the Agency of approved*
23 *State, local, Tribal, and territorial government employees*
24 *in cyber workforce positions.*

1 **SEC. 4. TITLE XXII TECHNICAL AND CLERICAL AMEND-**
2 **MENTS.**

3 (a) *TECHNICAL AMENDMENTS.*—

4 (1) *HOMELAND SECURITY ACT OF 2002.*—*Subtitle*
5 *A of title XXII of the Homeland Security Act of 2002*
6 *(6 U.S.C. 651 et seq.) is amended—*

7 (A) *in the first section 2215 (6 U.S.C. 665;*
8 *relating to the duties and authorities relating to*
9 *.gov internet domain), by amending the section*
10 *enumerator and heading to read as follows:*

11 **“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV**
12 **INTERNET DOMAIN.”;**

13 (B) *in the second section 2215 (6 U.S.C.*
14 *665b; relating to the joint cyber planning office),*
15 *by amending the section enumerator and head-*
16 *ing to read as follows:*

17 **“SEC. 2216. JOINT CYBER PLANNING OFFICE.”;**

18 (C) *in the third section 2215 (6 U.S.C.*
19 *665c; relating to the Cybersecurity State Coordi-*
20 *nator), by amending the section enumerator and*
21 *heading to read as follows:*

22 **“SEC. 2217. CYBERSECURITY STATE COORDINATOR.”;**

23 (D) *in the fourth section 2215 (6 U.S.C.*
24 *665d; relating to Sector Risk Management Agen-*
25 *cies), by amending the section enumerator and*
26 *heading to read as follows:*

1 **“SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.”;**

2 *(E) in section 2216 (6 U.S.C. 665e; relating*
 3 *to the Cybersecurity Advisory Committee), by*
 4 *amending the section enumerator and heading to*
 5 *read as follows:*

6 **“SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE.”; and**

7 *(F) in section 2217 (6 U.S.C. 665f; relating*
 8 *to Cybersecurity Education and Training Pro-*
 9 *grams), by amending the section enumerator and*
 10 *heading to read as follows:*

11 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING**
 12 **PROGRAMS.”.**

13 *(2) CONSOLIDATED APPROPRIATIONS ACT, 2021.—*
 14 *Paragraph (1) of section 904(b) of division U of the*
 15 *Consolidated Appropriations Act, 2021 (Public Law*
 16 *116–260) is amended, in the matter preceding sub-*
 17 *paragraph (A), by inserting “of 2002” after “Home-*
 18 *land Security Act”.*

19 *(b) CLERICAL AMENDMENT.—The table of contents in*
 20 *section 1(b) of the Homeland Security Act of 2002 is*
 21 *amended by striking the items relating to sections 2214*
 22 *through 2217 and inserting the following new items:*

“Sec. 2214. National Asset Database.

“Sec. 2215. Duties and authorities relating to .gov internet domain.

“Sec. 2216. Joint cyber planning office.

“Sec. 2217. Cybersecurity State Coordinator.

“Sec. 2218. Sector Risk Management Agencies.

“Sec. 2219. Cybersecurity Advisory Committee.

“Sec. 2220. Cybersecurity Education and Training Programs.”.

Union Calendar No. 31

117TH CONGRESS
1ST Session

H. R. 3138

[Report No. 117-48]

A BILL

To amend the Homeland Security Act of 2002 to authorize a grant program relating to the cybersecurity of State and local governments, and for other purposes.

JUNE 1, 2021

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed