

117TH CONGRESS
1ST SESSION

S. 2585

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

IN THE SENATE OF THE UNITED STATES

AUGUST 3, 2021

Ms. HASSAN (for herself, Mr. CORNYN, Ms. SINEMA, and Mr. TILLIS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To amend the Homeland Security Act of 2002 to authorize a grant program relating to the cybersecurity of State, local, Tribal, and territorial 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 Cyber-
5 security Improvement Act”.

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

3 (a) IN GENERAL.—Subtitle A of title XXII of the
 4 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)
 5 is amended by adding at the end the following:

6 **“SEC. 2218. STATE AND LOCAL CYBERSECURITY GRANT**
 7 **PROGRAM.**

8 “(a) DEFINITIONS.—In this section:

9 “(1) APPROPRIATE COMMITTEES OF CON-
 10 GRESS.—The term ‘appropriate committees of Con-
 11 gress’ means—

12 “(A) the Committee on Homeland Security
 13 and Governmental Affairs of the Senate; and

14 “(B) the Committee on Homeland Security
 15 of the House of Representatives.

16 “(2) CYBER THREAT INDICATOR.—The term
 17 ‘cyber threat indicator’ has the meaning given the
 18 term in section 102 of the Cybersecurity Act of 2015
 19 (6 U.S.C. 1501).

20 “(3) CYBERSECURITY PLAN.—The term ‘Cyber-
 21 security Plan’ means a plan submitted by an eligible
 22 entity under subsection (e)(1).

23 “(4) ELIGIBLE ENTITY.—The term ‘eligible en-
 24 tity’ means a—

25 “(A) State; or

26 “(B) Tribal government.

1 “(5) INCIDENT.—The term ‘incident’ has the
2 meaning given the term in section 2209.

3 “(6) INFORMATION SHARING AND ANALYSIS OR-
4 GANIZATION.—The term ‘information sharing and
5 analysis organization’ has the meaning given the
6 term in section 2222.

7 “(7) INFORMATION SYSTEM.—The term ‘infor-
8 mation system’ has the meaning given the term in
9 section 102 of the Cybersecurity Act of 2015 (6
10 U.S.C. 1501).

11 “(8) MULTI-ENTITY GROUP.—The term ‘multi-
12 entity group’ means a group of 2 or more eligible
13 entities desiring a grant under this section.

14 “(9) ONLINE SERVICE.—The term ‘online serv-
15 ice’ means any internet-facing service, including a
16 website, email, virtual private network, or custom
17 application.

18 “(10) RURAL AREA.—The term ‘rural area’ has
19 the meaning given the term in section 5302 of title
20 49, United States Code.

21 “(11) STATE AND LOCAL CYBERSECURITY
22 GRANT PROGRAM.—The term ‘State and Local Cy-
23 bersecurity Grant Program’ means the program es-
24 tablished under subsection (b).

1 “(12) TRIBAL GOVERNMENT.—The term ‘Tribal
2 government’ means the recognized governing body of
3 any Indian or Alaska Native Tribe, band, nation,
4 pueblo, village, community, component band, or com-
5 ponent reservation, that is individually identified (in-
6 cluding parenthetically) in the most recent list pub-
7 lished pursuant to Section 104 of the Federally Rec-
8 ognized Indian Tribe List Act of 1994 (25 U.S.C.
9 5131).

10 “(b) ESTABLISHMENT.—

11 “(1) IN GENERAL.—There is established within
12 the Department a program to award grants to eligi-
13 ble entities to address cybersecurity risks and cyber-
14 security threats to information systems owned or op-
15 erated by, or on behalf of, State, local, or Tribal
16 governments.

17 “(2) APPLICATION.—An eligible entity desiring
18 a grant under the State and Local Cybersecurity
19 Grant Program shall submit to the Secretary an ap-
20 plication at such time, in such manner, and con-
21 taining such information as the Secretary may re-
22 quire.

23 “(c) ADMINISTRATION.—The State and Local Cyber-
24 security Grant Program shall be administered in the same

1 office of the Department that administers grants made
2 under sections 2003 and 2004.

3 “(d) USE OF FUNDS.—An eligible entity that receives
4 a grant under this section and a local government that
5 receives funds from a grant under this section, as appro-
6 priate, shall use the grant to—

7 “(1) implement the Cybersecurity Plan of the
8 eligible entity;

9 “(2) develop or revise the Cybersecurity Plan of
10 the eligible entity;

11 “(3) pay expenses directly relating to the ad-
12 ministration of the grant, which shall not exceed 5
13 percent of the amount of the grant;

14 “(4) assist with activities that address immi-
15 nent cybersecurity threats, as confirmed by the Sec-
16 retary, acting through the Director, to the informa-
17 tion systems owned or operated by, or on behalf of,
18 the eligible entity or a local government within the
19 jurisdiction of the eligible entity; or

20 “(5) fund any other appropriate activity deter-
21 mined by the Secretary, acting through the Director.

22 “(e) CYBERSECURITY PLANS.—

23 “(1) IN GENERAL.—An eligible entity applying
24 for a grant under this section shall submit to the

1 Secretary a Cybersecurity Plan for review in accord-
2 ance with subsection (i).

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

5 “(A) incorporate, to the extent prac-
6 ticable—

7 “(i) any existing plans of the eligible
8 entity to protect against cybersecurity risks
9 and cybersecurity threats to information
10 systems owned or operated by, or on behalf
11 of, State, local, or Tribal governments; and

12 “(ii) if the eligible entity is a State,
13 consultation and feedback from local gov-
14 ernments and associations of local govern-
15 ments within the jurisdiction of the eligible
16 entity;

17 “(B) describe, to the extent practicable,
18 how the eligible entity will—

19 “(i) manage, monitor, and track infor-
20 mation systems, applications, and user ac-
21 counts owned or operated by, or on behalf
22 of, the eligible entity or, if the eligible enti-
23 ty is a State, local governments within the
24 jurisdiction of the eligible entity, and the
25 information technology deployed on those

1 information systems, including legacy in-
2 formation systems and information tech-
3 nology that are no longer supported by the
4 manufacturer of the systems or technology;

5 “(ii) monitor, audit, and, track net-
6 work traffic and activity transiting or trav-
7 eling to or from information systems, ap-
8 plications, and user accounts owned or op-
9 erated by, or on behalf of, the eligible enti-
10 ty or, if the eligible entity is a State, local
11 governments within the jurisdiction of the
12 eligible entity;

13 “(iii) enhance the preparation, re-
14 sponse, and resiliency of information sys-
15 tems, applications, and user accounts
16 owned or operated by, or on behalf of, the
17 eligible entity or, if the eligible entity is a
18 State, local governments within the juris-
19 diction of the eligible entity, against cyber-
20 security risks and cybersecurity threats;

21 “(iv) implement a process of contin-
22 uous cybersecurity vulnerability assess-
23 ments and threat mitigation practices
24 prioritized by degree of risk to address cy-
25 bersecurity risks and cybersecurity threats

1 on information systems, applications, and
2 user accounts owned or operated by, or on
3 behalf of, the eligible entity or, if the eligi-
4 ble entity is a State, local governments
5 within the jurisdiction of the eligible entity;

6 “(v) ensure that the eligible entity
7 and, if the eligible entity is a State, local
8 governments within the jurisdiction of the
9 eligible entity, adopt and use best practices
10 and methodologies to enhance cybersecu-
11 rity, such as—

12 “(I) the practices set forth in the
13 cybersecurity framework developed by
14 the National Institute of Standards
15 and Technology;

16 “(II) cyber chain supply chain
17 risk management best practices iden-
18 tified by the National Institute of
19 Standards and Technology; and

20 “(III) knowledge bases of adver-
21 sary tools and tactics;

22 “(vi) promote the delivery of safe, rec-
23 ognizable, and trustworthy online services
24 by the eligible entity and, if the eligible en-
25 tity is a State, local governments within

1 the jurisdiction of the eligible entity, in-
2 cluding through the use of the .gov inter-
3 net domain;

4 “(vii) ensure continuity of operations
5 of the eligible entity and, if the eligible en-
6 tity is a State, local governments within
7 the jurisdiction of the eligible entity, in the
8 event of a cybersecurity incident, including
9 by conducting exercises to practice re-
10 sponding to a cybersecurity incident;

11 “(viii) use the National Initiative for
12 Cybersecurity Education Workforce
13 Framework for Cybersecurity developed by
14 the National Institute of Standards and
15 Technology to identify and mitigate any
16 gaps in the cybersecurity workforces of the
17 eligible entity and, if the eligible entity is
18 a State, local governments within the juris-
19 diction of the eligible entity, enhance re-
20 cruitment and retention efforts for those
21 workforces, and bolster the knowledge,
22 skills, and abilities of personnel of the eli-
23 gible entity and, if the eligible entity is a
24 State, local governments within the juris-
25 diction of the eligible entity, to address cy-

bersecurity risks and cybersecurity threats,
such as through cybersecurity hygiene
training;

“(ix) if the eligible entity is a State,
ensure continuity of communications and
data networks within the jurisdiction of the
eligible entity between the eligible entity
and local governments within the jurisdic-
tion of the eligible entity in the event of an
incident involving those communications or
data networks;

“(x) assess and mitigate, to the great-
est degree possible, cybersecurity risks and
cybersecurity threats relating to critical in-
frastructure and key resources, the deg-
radation of which may impact the perform-
ance of information systems within the ju-
risdiction of the eligible entity;

“(xi) enhance capabilities to share
cyber threat indicators and related infor-
mation between the eligible entity and—

“(I) if the eligible entity is a
State, local governments within the
jurisdiction of the eligible entity, in-
cluding by expanding information

1 sharing agreements with the Depart-
2 ment; and

3 “(II) the Department;

4 “(xii) leverage cybersecurity services
5 offered by the Department;

6 “(xiii) implement an information tech-
7 nology and operational technology mod-
8 ernization cybersecurity review process
9 that ensures alignment between informa-
10 tion technology and operational technology
11 cybersecurity objectives;

12 “(xiv) develop and coordinate strate-
13 gies to address cybersecurity risks and cy-
14 bersecurity threats in consultation with—

15 “(I) if the eligible entity is a
16 State, local governments and associa-
17 tions of local governments within the
18 jurisdiction of the eligible entity; and

19 “(II) as applicable—

20 “(aa) eligible entities that
21 neighbor the jurisdiction of the
22 eligible entity or, as appropriate,
23 members of an information shar-
24 ing and analysis organization;
25 and

1 “(bb) countries that neigh-
2 bor the jurisdiction of the eligible
3 entity;

4 “(xv) ensure adequate access to, and
5 participation in, the services and programs
6 described in this subparagraph by rural
7 areas within the jurisdiction of the eligible
8 entity; and

9 “(xvi) distribute funds, items, serv-
10 ices, capabilities, or activities to local gov-
11 ernments under subsection (n)(2)(A), in-
12 cluding the fraction of that distribution the
13 eligible entity plans to distribute to rural
14 areas under subsection (n)(2)(B);

15 “(C) assess the capabilities of the eligible
16 entity relating to the actions described in sub-
17 paragraph (B);

18 “(D) describe, as appropriate and to the
19 extent practicable, the individual responsibilities
20 of the eligible entity and local governments
21 within the jurisdiction of the eligible entity in
22 implementing the plan;

23 “(E) outline, to the extent practicable, the
24 necessary resources and a timeline for imple-
25 menting the plan; and

1 “(F) describe the metrics the eligible entity
2 will use to measure progress towards—

3 “(i) implementing the plan; and

4 “(ii) reducing cybersecurity risks to,
5 and identifying, responding to, and recov-
6 ering from cybersecurity threats to, infor-
7 mation systems owned or operated by, or
8 on behalf of, the eligible entity or, if the el-
9 igible entity is a State, local governments
10 within the jurisdiction of the eligible entity.

11 “(3) DISCRETIONARY ELEMENTS.—In drafting
12 a Cybersecurity Plan, an eligible entity may—

13 “(A) consult with the Multi-State Informa-
14 tion Sharing and Analysis Center;

15 “(B) include a description of cooperative
16 programs developed by groups of local govern-
17 ments within the jurisdiction of the eligible en-
18 tity to address cybersecurity risks and cyberse-
19 curity threats; and

20 “(C) include a description of programs
21 provided by the eligible entity to support local
22 governments and owners and operators of crit-
23 ical infrastructure to address cybersecurity
24 risks and cybersecurity threats.

25 “(f) MULTI-ENTITY GRANTS.—

1 “(1) IN GENERAL.—The Secretary may award
2 grants under this section to a multi-entity group to
3 support multi-entity efforts to address cybersecurity
4 risks and cybersecurity threats to information sys-
5 tems within the jurisdictions of the eligible entities
6 that comprise the multi-entity group.

7 “(2) SATISFACTION OF OTHER REQUIRE-
8 MENTS.—In order to be eligible for a multi-entity
9 grant under this subsection, each eligible entity that
10 comprises a multi-entity group shall have—

11 “(A) a Cybersecurity Plan that has been
12 reviewed by the Secretary in accordance with
13 subsection (i); and

14 “(B) a cybersecurity planning committee
15 established in accordance with subsection (g).

16 “(3) APPLICATION.—

17 “(A) IN GENERAL.—A multi-entity group
18 applying for a multi-entity grant under para-
19 graph (1) shall submit to the Secretary an ap-
20 plication at such time, in such manner, and
21 containing such information as the Secretary
22 may require.

23 “(B) MULTI-ENTITY PROJECT PLAN.—An
24 application for a grant under this section of a

1 multi-entity group under subparagraph (A)
 2 shall include a plan describing—

3 “(i) the division of responsibilities
 4 among the eligible entities that comprise
 5 the multi-entity group;

6 “(ii) the distribution of funding from
 7 the grant among the eligible entities that
 8 comprise the multi-entity group; and

9 “(iii) how the eligible entities that
 10 comprise the multi-entity group will work
 11 together to implement the Cybersecurity
 12 Plan of each of those eligible entities.

13 “(g) PLANNING COMMITTEES.—

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

17 “(A) assist with the development, imple-
 18 mentation, and revision of the Cybersecurity
 19 Plan of the eligible entity;

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

22 “(C) assist with the determination of effec-
 23 tive funding priorities for a grant under this
 24 section in accordance with subsections (d) and
 25 (j).

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

3 “(A) be comprised of representatives
4 from—

5 “(i) the eligible entity;

6 “(ii) if the eligible entity is a State,
7 counties, cities, and towns within the juris-
8 diction of the eligible entity; and

9 “(iii) institutions of public education
10 and health within the jurisdiction of the el-
11 igible entity; and

12 “(B) include, as appropriate, representa-
13 tives of rural, suburban, and high-population
14 jurisdictions.

15 “(3) CYBERSECURITY EXPERTISE.—Not less
16 than one-half of the representatives of a committee
17 established under paragraph (1) shall have profes-
18 sional experience relating to cybersecurity or infor-
19 mation technology.

20 “(4) RULE OF CONSTRUCTION REGARDING EX-
21 ISTING PLANNING COMMITTEES.—Nothing in this
22 subsection shall be construed to require an eligible
23 entity to establish a cybersecurity planning com-
24 mittee if the eligible entity has established and uses

1 a multijurisdictional planning committee or commis-
2 sion that—

3 “(A) meets the requirements of this sub-
4 section; or

5 “(B) may be expanded or leveraged to
6 meet the requirements of this subsection, in-
7 cluding through the formation of a cybersecu-
8 rity planning subcommittee.

9 “(5) RULE OF CONSTRUCTION REGARDING CON-
10 TROL OF INFORMATION SYSTEMS OF ELIGIBLE ENTI-
11 TIES.—Nothing in this subsection shall be construed
12 to permit a cybersecurity planning committee of an
13 eligible entity that meets the requirements of this
14 subsection to make decisions relating to information
15 systems owned or operated by, or on behalf of, the
16 eligible entity.

17 “(h) SPECIAL RULE FOR TRIBAL GOVERNMENTS.—
18 With respect to any requirement under subsection (e) or
19 (g), the Secretary, in consultation with the Secretary of
20 the Interior and Tribal governments, may prescribe an al-
21 ternative substantively similar requirement for Tribal gov-
22 ernments if the Secretary finds that the alternative re-
23 quirement is necessary for the effective delivery and ad-
24 ministration of grants to Tribal governments under this
25 section.

1 “(i) REVIEW OF PLANS.—

2 “(1) REVIEW AS CONDITION OF GRANT.—

3 “(A) IN GENERAL.—Subject to paragraph
4 (3), before an eligible entity may receive a
5 grant under this section, the Secretary, acting
6 through the Director, shall—

7 “(i) review the Cybersecurity Plan of
8 the eligible entity, including any revised
9 Cybersecurity Plans of the eligible entity;
10 and

11 “(ii) determine that the Cybersecurity
12 Plan reviewed under clause (i) satisfies the
13 requirements under paragraph (2).

14 “(B) DURATION OF DETERMINATION.—In
15 the case of a determination under subparagraph
16 (A)(ii) that a Cybersecurity Plan satisfies the
17 requirements under paragraph (2), the deter-
18 mination shall be effective for the 2-year period
19 beginning on the date of the determination.

20 “(C) ANNUAL RENEWAL.—Not later than
21 2 years after the date on which the Secretary
22 determines under subparagraph (A)(ii) that a
23 Cybersecurity Plan satisfies the requirements
24 under paragraph (2), and annually thereafter,

1 the Secretary, acting through the Director,
2 shall—

3 “(i) determine whether the Cybersecu-
4 rity Plan and any revisions continue to
5 meet the criteria described in paragraph
6 (2); and

7 “(ii) renew the determination if the
8 Secretary, acting through the Director,
9 makes a positive determination under
10 clause (i).

11 “(2) PLAN REQUIREMENTS.—In reviewing a
12 Cybersecurity Plan of an eligible entity under this
13 subsection, the Secretary, acting through the Direc-
14 tor, shall ensure that the Cybersecurity Plan—

15 “(A) satisfies the requirements of sub-
16 section (e)(2); and

17 “(B) has been approved by—

18 “(i) the cybersecurity planning com-
19 mittee of the eligible entity established
20 under subsection (g); and

21 “(ii) the Chief Information Officer,
22 the Chief Information Security Officer, or
23 an equivalent official of the eligible entity.

24 “(3) EXCEPTION.—Notwithstanding subsection
25 (e) and paragraph (1) of this subsection, the Sec-

1 retary may award a grant under this section to an
 2 eligible entity that does not submit a Cybersecurity
 3 Plan to the Secretary for review before September
 4 30, 2023, if the eligible entity certifies to the Sec-
 5 retary that—

6 “(A) the activities that will be supported
 7 by the grant are—

8 “(i) integral to the development of the
 9 Cybersecurity Plan of the eligible entity; or

10 “(ii) necessary to assist with activities
 11 described in subsection (d)(4), as con-
 12 firmed by the Director; and

13 “(B) the eligible entity will submit to the
 14 Secretary a Cybersecurity Plan for review under
 15 this subsection by September 30, 2023.

16 “(4) RULE OF CONSTRUCTION.—Nothing in
 17 this subsection shall be construed to provide author-
 18 ity to the Secretary to—

19 “(A) regulate the manner by which an eli-
 20 gible entity or local government improves the
 21 cybersecurity of the information systems owned
 22 or operated by, or on behalf of, the eligible enti-
 23 ty or local government; or

24 “(B) condition the receipt of grants under
 25 this section on—

1 “(i) participation in a particular Fed-
2 eral program; or

3 “(ii) the use of a specific product or
4 technology.

5 “(j) LIMITATIONS ON USES OF FUNDS.—

6 “(1) IN GENERAL.—Any entity that receives
7 funds from a grant under this section may not use
8 the grant—

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

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

12 “(C) to pay a ransom;

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

14 “(E) for any purpose that does not address
15 cybersecurity risks or cybersecurity threats on
16 information systems owned or operated by, or
17 on behalf of, the eligible entity that receives the
18 grant or a local government within the jurisdic-
19 tion of the eligible entity.

20 “(2) COMPLIANCE OVERSIGHT.—In addition to
21 any other remedy available, the Secretary may take
22 such actions as are necessary to ensure that a recipi-
23 ent of a grant under this section uses the grant for
24 the purposes for which the grant is awarded.

1 “(3) RULE OF CONSTRUCTION.—Nothing in
2 paragraph (1)(A) shall be construed to prohibit the
3 use of funds from a grant under this section award-
4 ed to a State, local, or Tribal government for other-
5 wise permissible uses under this section on the basis
6 that the State, local, or Tribal government has pre-
7 viously used State, local, or Tribal funds to support
8 the same or similar uses.

9 “(k) OPPORTUNITY TO AMEND APPLICATIONS.—In
10 considering applications for grants under this section, the
11 Secretary shall provide applicants with a reasonable op-
12 portunity to correct any defects in those applications be-
13 fore making final awards, including by allowing applicants
14 to revise a submitted Cybersecurity Plan.

15 “(l) APPORTIONMENT.—For fiscal year 2022 and
16 each fiscal year thereafter, the Secretary shall apportion
17 amounts appropriated to carry out this section among eli-
18 gible entities as follows:

19 “(1) BASELINE AMOUNT.—The Secretary shall
20 first apportion—

21 “(A) 0.25 percent of such amounts to each
22 of American Samoa, the Commonwealth of the
23 Northern Mariana Islands, Guam, and the
24 United States Virgin Islands;

1 “(B) 1 percent of such amounts to each of
2 the remaining States; and

3 “(C) 3 percent of such amounts to Tribal
4 governments.

5 “(2) REMAINDER.—The Secretary shall appor-
6 tion the remainder of such amounts to States as fol-
7 lows:

8 “(A) 50 percent of such remainder in the
9 ratio that the population of each State, bears to
10 the population of all States; and

11 “(B) 50 percent of such remainder in the
12 ratio that the population of each State that re-
13 sides in rural areas, bears to the population of
14 all States that resides in rural areas.

15 “(3) APPORTIONMENT AMONG TRIBAL GOVERN-
16 MENTS.—In determining how to apportion amounts
17 to Tribal governments under paragraph (1)(C), the
18 Secretary shall consult with the Secretary of the In-
19 terior and Tribal governments.

20 “(4) MULTI-ENTITY GRANTS.—An amount re-
21 ceived from a multi-entity grant awarded under sub-
22 section (f)(1) by a State or Tribal government that
23 is a member of the multi-entity group shall qualify
24 as an apportionment for the purpose of this sub-
25 section.

1 “(m) FEDERAL SHARE.—

2 “(1) IN GENERAL.—The Federal share of the
3 cost of an activity carried out using funds made
4 available with a grant under this section may not ex-
5 ceed—

6 “(A) in the case of a grant to an eligible
7 entity—

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

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

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

11 and

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

13 and

14 “(B) in the case of a grant to a multi-enti-
15 ty group—

16 “(i) for fiscal year 2022, 100 percent;

17 “(ii) for fiscal year 2023, 90 percent;

18 “(iii) for fiscal year 2024, 80 percent;

19 and

20 “(iv) for fiscal year 2025, 70 percent.

21 “(2) WAIVER.—

22 “(A) IN GENERAL.—The Secretary may
23 waive or modify the requirements of paragraph
24 (1) if an eligible entity or multi-entity group
25 demonstrates economic hardship.

1 “(B) GUIDELINES.—The Secretary shall
2 establish and publish guidelines for determining
3 what constitutes economic hardship for the pur-
4 poses of this subsection.

5 “(C) CONSIDERATIONS.—In developing
6 guidelines under subparagraph (B), the Sec-
7 retary shall consider, with respect to the juris-
8 diction of an eligible entity—

9 “(i) changes in rates of unemployment
10 in the jurisdiction from previous years;

11 “(ii) changes in the percentage of in-
12 dividuals who are eligible to receive bene-
13 fits under the supplemental nutrition as-
14 sistance program established under the
15 Food and Nutrition Act of 2008 (7 U.S.C.
16 2011 et seq.) from previous years; and

17 “(iii) any other factors the Secretary
18 considers appropriate.

19 “(3) WAIVER FOR TRIBAL GOVERNMENTS.—
20 Notwithstanding paragraph (2), the Secretary, in
21 consultation with the Secretary of the Interior and
22 Tribal governments, may waive or modify the re-
23 quirements of paragraph (1) for 1 or more Tribal
24 governments if the Secretary determines that the
25 waiver is in the public interest.

1 “(n) RESPONSIBILITIES OF GRANTEES.—

2 “(1) CERTIFICATION.—Each eligible entity or
3 multi-entity group that receives a grant under this
4 section shall certify to the Secretary that the grant
5 will be used—

6 “(A) for the purpose for which the grant
7 is awarded; and

8 “(B) in compliance with subsections (d)
9 and (j).

10 “(2) AVAILABILITY OF FUNDS TO LOCAL GOV-
11 ERNMENTS AND RURAL AREAS.—

12 “(A) IN GENERAL.—Subject to subpara-
13 graph (C), not later than 45 days after the date
14 on which an eligible entity or multi-entity group
15 receives a grant under this section, the eligible
16 entity or multi-entity group shall, without im-
17 posing unreasonable or unduly burdensome re-
18 quirements as a condition of receipt, obligate or
19 otherwise make available to local governments
20 within the jurisdiction of the eligible entity or
21 the eligible entities that comprise the multi-enti-
22 ty group, consistent with the Cybersecurity
23 Plan of the eligible entity or the Cybersecurity
24 Plans of the eligible entities that comprise the
25 multi-entity group—

1 “(i) not less than 80 percent of funds
2 available under the grant;

3 “(ii) with the consent of the local gov-
4 ernments, items, services, capabilities, or
5 activities having a value of not less than
6 80 percent of the amount of the grant; or

7 “(iii) with the consent of the local
8 governments, grant funds combined with
9 other items, services, capabilities, or activi-
10 ties having the total value of not less than
11 80 percent of the amount of the grant.

12 “(B) AVAILABILITY TO RURAL AREAS.—In
13 obligating funds, items, services, capabilities, or
14 activities to local governments under subpara-
15 graph (A), the eligible entity or eligible entities
16 that comprise the multi-entity group shall en-
17 sure that rural areas within the jurisdiction of
18 the eligible entity or the eligible entities that
19 comprise the multi-entity group receive not less
20 than—

21 “(i) 25 percent of the amount of the
22 grant awarded to the eligible entity;

23 “(ii) items, services, capabilities, or
24 activities having a value of not less than

25 percent of the amount of the grant
awarded to the eligible entity; or

“(iii) grant funds combined with other
items, services, capabilities, or activities
having the total value of not less than 25
percent of the grant awarded to the eligible
entity.

“(C) EXCEPTIONS.—This paragraph shall
not apply to—

“(i) any grant awarded under this
section that solely supports activities that
are integral to the development or revision
of the Cybersecurity Plan of the eligible
entity; or

“(ii) the District of Columbia, the
Commonwealth of Puerto Rico, American
Samoa, the Commonwealth of the North-
ern Mariana Islands, Guam, the United
States Virgin Islands, or a Tribal govern-
ment.

“(3) CERTIFICATIONS REGARDING DISTRIBU-
TION OF GRANT FUNDS TO LOCAL GOVERNMENTS.—
An eligible entity or multi-entity group shall certify
to the Secretary that the eligible entity or multi-enti-

1 ty group has made the distribution to local govern-
2 ments required under paragraph (2).

3 “(4) EXTENSION OF PERIOD.—

4 “(A) IN GENERAL.—An eligible entity or
5 multi-entity group may request in writing that
6 the Secretary extend the period of time speci-
7 fied in paragraph (2) for an additional period
8 of time.

9 “(B) APPROVAL.—The Secretary may ap-
10 prove a request for an extension under subpara-
11 graph (A) if the Secretary determines the ex-
12 tension is necessary to ensure that the obliga-
13 tion and expenditure of grant funds align with
14 the purpose of the State and Local Cybersecu-
15 rity Grant Program.

16 “(5) DIRECT FUNDING.—If an eligible entity
17 does not make a distribution to a local government
18 required under paragraph (2) in a timely fashion,
19 the local government may petition the Secretary to
20 request the Secretary to provide funds directly to the
21 local government.

22 “(6) LIMITATION ON CONSTRUCTION.—A grant
23 awarded under this section may not be used to ac-
24 quire land or to construct, remodel, or perform alter-
25 ations of buildings or other physical facilities.

1 “(7) CONSULTATION IN ALLOCATING FUNDS.—

2 An eligible entity applying for a grant under this
 3 section shall agree to consult the Chief Information
 4 Officer, the Chief Information Security Officer, or
 5 an equivalent official of the eligible entity in allo-
 6 cating funds from a grant awarded under this sec-
 7 tion.

8 “(8) PENALTIES.—In addition to other rem-
 9 edies available to the Secretary, if an eligible entity
 10 violates a requirement of this subsection, the Sec-
 11 retary may—

12 “(A) terminate or reduce the amount of a
 13 grant awarded under this section to the eligible
 14 entity; or

15 “(B) distribute grant funds previously
 16 awarded to the eligible entity—

17 “(i) in the case of an eligible entity
 18 that is a State, directly to the appropriate
 19 local government as a replacement grant in
 20 an amount determined by the Secretary; or

21 “(ii) in the case of an eligible entity
 22 that is a Tribal government, to another
 23 Tribal government or Tribal governments
 24 as a replacement grant in an amount de-
 25 termined by the Secretary.

1 “(o) CONSULTATION WITH STATE, LOCAL, AND
2 TRIBAL REPRESENTATIVES.—In carrying out this section,
3 the Secretary shall consult with State, local, and Tribal
4 representatives with professional experience relating to cy-
5 bersecurity, including representatives of associations rep-
6 resenting State, local, and Tribal governments, to in-
7 form—

8 “(1) guidance for applicants for grants under
9 this section, including guidance for Cybersecurity
10 Plans;

11 “(2) the study of risk-based formulas required
12 under subsection (q)(4);

13 “(3) the development of guidelines required
14 under subsection (m)(2)(B); and

15 “(4) any modifications described in subsection
16 (q)(2)(D).

17 “(p) NOTIFICATION TO CONGRESS.—Not later than
18 3 business days before the date on which the Department
19 announces the award of a grant to an eligible entity under
20 this section, including an announcement to the eligible en-
21 tity, the Secretary shall provide to the appropriate com-
22 mittees of Congress notice of the announcement.

23 “(q) REPORTS, STUDY, AND REVIEW.—

24 “(1) ANNUAL REPORTS BY GRANT RECIPI-
25 ENTS.—

“(A) IN GENERAL.—Not later than 1 year after the date on which an eligible entity receives a grant under this section for the purpose of implementing the Cybersecurity Plan of the eligible entity, including an eligible entity that comprises a multi-entity group that receives a grant for that purpose, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report that, using the metrics described in the Cybersecurity Plan of the eligible entity, describes the progress of the eligible entity in—

“(i) implementing the Cybersecurity Plan of the eligible entity; and

“(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity.

“(B) ABSENCE OF PLAN.—Not later than 1 year after the date on which an eligible entity that does not have a Cybersecurity Plan re-

ceives funds under this section, and annually thereafter until 1 year after the date on which funds from the grant are expended or returned, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds to—

“(i) develop or revise a Cybersecurity Plan; or

“(ii) assist with the activities described in subsection (d)(4).

“(2) ANNUAL REPORTS TO CONGRESS.—Not less frequently than annually, the Secretary, acting through the Director, shall submit to Congress a report on—

“(A) the use of grants awarded under this section;

“(B) the proportion of grants used to support cybersecurity in rural areas;

“(C) the effectiveness of the State and Local Cybersecurity Grant Program;

“(D) any necessary modifications to the State and Local Cybersecurity Grant Program; and

“(E) any progress made toward—

1 “(i) developing, implementing, or re-
2 vising Cybersecurity Plans; and

3 “(ii) reducing cybersecurity risks to,
4 and identifying, responding to, and recov-
5 ering from cybersecurity threats to, infor-
6 mation systems owned or operated by, or
7 on behalf of, State, local, or Tribal govern-
8 ments as a result of the award of grants
9 under this section.

10 “(3) PUBLIC AVAILABILITY.—

11 “(A) IN GENERAL.—The Secretary, acting
12 through the Director, shall make each report
13 submitted under paragraph (2) publicly avail-
14 able, including by making each report available
15 on the website of the Agency.

16 “(B) REDACTIONS.—In making each re-
17 port publicly available under subparagraph (A),
18 the Director may make redactions that the Di-
19 rector, in consultation with each eligible entity,
20 determines necessary to protect classified or
21 other information exempt from disclosure under
22 section 552 of title 5, United States Code (com-
23 monly referred to as the ‘Freedom of Informa-
24 tion Act’).

25 “(4) STUDY OF RISK-BASED FORMULAS.—

1 “(A) IN GENERAL.—Not later than Sep-
2 tember 30, 2024, the Secretary, acting through
3 the Director, shall submit to the appropriate
4 committees of Congress a study and legislative
5 recommendations on the potential use of a risk-
6 based formula for apportioning funds under
7 this section, including—

8 “(i) potential components that could
9 be included in a risk-based formula, includ-
10 ing the potential impact of those compo-
11 nents on support for rural areas under this
12 section;

13 “(ii) potential sources of data and in-
14 formation necessary for the implementa-
15 tion of a risk-based formula;

16 “(iii) any obstacles to implementing a
17 risk-based formula, including obstacles
18 that require a legislative solution;

19 “(iv) if a risk-based formula were to
20 be implemented for fiscal year 2026, a rec-
21 ommended risk-based formula for the
22 State and Local Cybersecurity Grant Pro-
23 gram; and

24 “(v) any other information that the
25 Secretary, acting through the Director, de-

1 termines necessary to help Congress under-
2 stand the progress towards, and obstacles
3 to, implementing a risk-based formula.

4 “(B) INAPPLICABILITY OF PAPERWORK RE-
5 DUCTION ACT.—The requirements of chapter
6 35 of title 44, United States Code (commonly
7 referred to as the ‘Paperwork Reduction Act’),
8 shall not apply to any action taken to carry out
9 this paragraph.

10 “(5) TRIBAL CYBERSECURITY NEEDS RE-
11 PORT.—Not later than 2 years after the date of en-
12 actment of this section, the Secretary, acting
13 through the Director, shall submit to Congress a re-
14 port that—

15 “(A) describes the cybersecurity needs of
16 Tribal governments, which shall be determined
17 in consultation with the Secretary of the Inte-
18 rior and Tribal governments; and

19 “(B) includes any recommendations for ad-
20 dressing the cybersecurity needs of Tribal gov-
21 ernments, including any necessary modifications
22 to the State and Local Cybersecurity Grant
23 Program to better serve Tribal governments.

24 “(6) GAO REVIEW.—Not later than 3 years
25 after the date of enactment of this section, the

1 Comptroller General of the United States shall con-
 2 duct a review of the State and Local Cybersecurity
 3 Grant Program, including—

4 “(A) the grant selection process of the Sec-
 5 retary; and

6 “(B) a sample of grants awarded under
 7 this section.

8 “(r) AUTHORIZATION OF APPROPRIATIONS.—

9 “(1) IN GENERAL.—There are authorized to be
 10 appropriated for activities under this section—

11 “(A) for fiscal year 2022, \$200,000,000;

12 “(B) for fiscal year 2023, \$400,000,000;

13 “(C) for fiscal year 2024, \$300,000,000;

14 and

15 “(D) for fiscal year 2025, \$100,000,000.

16 “(2) TRANSFERS AUTHORIZED.—

17 “(A) IN GENERAL.—During a fiscal year,
 18 the Secretary or the head of any component of
 19 the Department that administers the State and
 20 Local Cybersecurity Grant Program may trans-
 21 fer not more than 5 percent of the amounts ap-
 22 propriated pursuant to paragraph (1) or other
 23 amounts appropriated to carry out the State
 24 and Local Cybersecurity Grant Program for
 25 that fiscal year to an account of the Depart-

1 ment for salaries, expenses, and other adminis-
 2 trative costs incurred for the management, ad-
 3 ministration, or evaluation of this section.

4 “(B) ADDITIONAL APPROPRIATIONS.—Any
 5 funds transferred under subparagraph (A) shall
 6 be in addition to any funds appropriated to the
 7 Department or the components described in
 8 subparagraph (A) for salaries, expenses, and
 9 other administrative costs.

10 “(s) TERMINATION.—

11 “(1) IN GENERAL.—Subject to paragraph (2),
 12 the requirements of this section shall terminate on
 13 September 30, 2025.

14 “(2) EXCEPTION.—The reporting requirements
 15 under subsection (q) shall terminate on the date that
 16 is 1 year after the date on which the final funds
 17 from a grant under this section are expended or re-
 18 turned.”.

19 (b) CLERICAL AMENDMENT.—The table of contents
 20 in section 1(b) of the Homeland Security Act of 2002
 21 (Public Law 107–296; 116 Stat. 2135), is amended by
 22 inserting after the item relating to section 2217 the fol-
 23 lowing:

“Sec. 2218. State and Local Cybersecurity Grant Program.”.

