

.....
(Original Signature of Member)

117TH CONGRESS
1ST SESSION

H. R. 3138

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

Ms. CLARKE of New York introduced the following bill; which was referred to the Committee on _____

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 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 new sec-
6 tions:

7 **“SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT**
8 **PROGRAM.**

9 “(a) DEFINITIONS.—In this section:

10 “(1) CYBER THREAT INDICATOR.—The term
11 ‘cyber threat indicator’ has the meaning given the
12 term in section 102 of the Cybersecurity Act of 2015
13 (6 U.S.C. 1501).

14 “(2) CYBERSECURITY PLAN.—The term ‘Cyber-
15 security Plan’ means a plan submitted by a State
16 under subsection (e)(1).

17 “(3) ELIGIBLE ENTITY.—The term ‘eligible en-
18 tity’ means—

19 “(A) a State; or

20 “(B) a federally recognized Indian Tribe
21 that, not later than 120 days after the date of
22 the enactment of this section or not later than
23 120 days before the start of any fiscal year in
24 which a grant under this section is awarded—

1 “(i) notifies the Secretary that the In-
2 dian Tribe intends to develop a Cybersecu-
3 rity Plan; and

4 “(ii) agrees to forfeit any distribution
5 under subsection (n)(2).

6 “(4) INCIDENT.—The term ‘incident’ has the
7 meaning given the term in section 2209.

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

12 “(6) INFORMATION SYSTEM.—The term ‘infor-
13 mation system’ has the meaning given the term in
14 section 102 of the Cybersecurity Act of 2015 (6
15 U.S.C. 1501).

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

20 “(9) STATE.—The term ‘State’ means each of
21 the several States, the District of Columbia, and the
22 territories and possessions of the United States.

23 “(10) STATE AND LOCAL CYBERSECURITY
24 GRANT PROGRAM.—The term ‘State and Local Cy-

1 bersecurity Grant Program’ means the program es-
2 tablished under subsection (b).

3 “(11) STATE AND LOCAL CYBERSECURITY RE-
4 SILIENCY COMMITTEE.—The term ‘State and Local
5 Cybersecurity Resiliency Committee’ means the com-
6 mittee established under subsection (o)(1).

7 “(b) ESTABLISHMENT.—

8 “(1) IN GENERAL.—The Secretary, acting
9 through the Director, shall establish a program, to
10 be known as the ‘the State and Local Cybersecurity
11 Grant Program’, to award grants to eligible entities
12 to address cybersecurity risks and cybersecurity
13 threats to information systems of State, local, or
14 Tribal governments.

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

21 “(c) BASELINE REQUIREMENTS.—An eligible entity
22 or multistate group that receives a grant under this sec-
23 tion shall use the grant in compliance with—

1 “(1) the Cybersecurity Plan of the eligible enti-
2 ty or the Cybersecurity Plans of the eligible entities
3 that comprise the multistate group; and

4 “(2) the Homeland Security Strategy to Im-
5 prove the Cybersecurity of State, Local, Tribal, and
6 Territorial Governments developed under section
7 2210(e)(1).

8 “(d) ADMINISTRATION.—The State and Local Cyber-
9 security Grant Program shall be administered in the same
10 office of the Department that administers grants made
11 under sections 2003 and 2004.

12 “(e) CYBERSECURITY PLANS.—

13 “(1) IN GENERAL.—An eligible entity applying
14 for a grant under this section shall submit to the
15 Secretary a Cybersecurity Plan for approval.

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

18 “(A) incorporate, to the extent practicable,
19 any existing plans of the eligible entity to pro-
20 tect against cybersecurity risks and cybersecu-
21 rity threats to information systems of State,
22 local, or Tribal governments;

23 “(B) describe, to the extent practicable,
24 how the eligible entity will—

1 “(i) manage, monitor, and track infor-
2 mation systems owned or operated by the
3 eligible entity or by local or Tribal govern-
4 ments within the jurisdiction of the eligible
5 entity and the information technology de-
6 ployed on those information systems, in-
7 cluding legacy information systems and in-
8 formation technology that are no longer
9 supported by the manufacturer of the sys-
10 tems or technology;

11 “(ii) monitor activity between infor-
12 mation systems owned or operated by the
13 eligible entity or by local or Tribal govern-
14 ments within the jurisdiction of the eligible
15 entity and between those information sys-
16 tems and information systems not owned
17 or operated by the eligible entity or by
18 local or Tribal governments within the ju-
19 risdiction of the eligible entity;

20 “(iii) enhance the preparation, re-
21 sponse, and resiliency of information sys-
22 tems owned or operated by the eligible en-
23 tity or local or Tribal governments against
24 cybersecurity risks and cybersecurity
25 threats;

1 “(iv) implement a process of contin-
2 uous cybersecurity vulnerability assess-
3 ments and threat mitigation practices
4 prioritized by degree of risk to address cy-
5 bersecurity risks and cybersecurity threats
6 on information systems of the eligible enti-
7 ty or local or Tribal governments;

8 “(v) ensure that State, local, and
9 Tribal governments that own or operate in-
10 formation systems that are located within
11 the jurisdiction of the eligible entity adopt
12 best practices and methodologies to en-
13 hance cybersecurity, such as the practices
14 set forth in the cybersecurity framework
15 developed by, and the cyber supply chain
16 risk management best practices identified
17 by, the National Institute of Standards
18 and Technology;

19 “(vi) promote the delivery of safe, rec-
20 ognizable, and trustworthy online services
21 by State, local, and Tribal governments,
22 including through the use of the .gov inter-
23 net domain;

24 “(vii) ensure continuity of operations
25 of the eligible entity and local, and Tribal

1 governments in the event of a cybersecu-
2 rity incident, including by conducting exer-
3 cises to practice responding to an incident;

4 “(viii) use the National Initiative for
5 Cybersecurity Education Cybersecurity
6 Workforce Framework developed by the
7 National Institute of Standards and Tech-
8 nology to identify and mitigate any gaps in
9 the cybersecurity workforces of State,
10 local, or Tribal governments, enhance re-
11 cruitment and retention efforts for such
12 workforces, and bolster the knowledge,
13 skills, and abilities of State, local, and
14 Tribal government personnel to address cy-
15 bersecurity risks and cybersecurity threats,
16 such as through cybersecurity hygiene
17 training;

18 “(ix) ensure continuity of communica-
19 tions and data networks within the juris-
20 diction of the eligible entity between the el-
21 igible entity and local and Tribal govern-
22 ments that own or operate information sys-
23 tems within the jurisdiction of the eligible
24 entity in the event of an incident involving

1 such communications or data networks
2 within the jurisdiction of the eligible entity;

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

10 “(xi) enhance capabilities to share
11 cyber threat indicators and related infor-
12 mation between the eligible entity and local
13 and Tribal governments that own or oper-
14 ate information systems within the juris-
15 diction of the eligible entity;

16 “(xii) enhance the capability of the el-
17 igible entity to share cyber threat indictors
18 and related information with the Depart-
19 ment;

20 “(xiii) leverage cybersecurity services
21 offered by the Department; and

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

1 “(I) local and Tribal govern-
2 ments within the jurisdiction of the el-
3 igible entity; and

4 “(II) as applicable—

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

10 “(bb) countries that neigh-
11 bor the jurisdiction of the eligible
12 entity;

13 “(C) describe, to the extent practicable, the
14 individual responsibilities of the eligible entity
15 and local and Tribal governments within the ju-
16 risdiction of the eligible entity in implementing
17 the plan;

18 “(D) outline, to the extent practicable, the
19 necessary resources and a timeline for imple-
20 menting the plan; and

21 “(E) describe how the eligible entity will
22 measure progress towards implementing the
23 plan.

1 “(3) DISCRETIONARY ELEMENTS.—A Cyberse-
2 curity Plan of an eligible entity may include a de-
3 scription of—

4 “(A) cooperative programs developed by
5 groups of local and Tribal governments within
6 the jurisdiction of the eligible entity to address
7 cybersecurity risks and cybersecurity threats;
8 and

9 “(B) programs provided by the eligible en-
10 tity to support local and Tribal governments
11 and owners and operators of critical infrastruc-
12 ture to address cybersecurity risks and cyberse-
13 curity threats.

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

21 “(f) MULTISTATE GRANTS.—

22 “(1) IN GENERAL.—The Secretary, acting
23 through the Director, may award grants under this
24 section to a group of two or more eligible entities to
25 support multistate efforts to address cybersecurity

1 risks and cybersecurity threats to information sys-
2 tems within the jurisdictions of the eligible entities.

3 “(2) SATISFACTION OF OTHER REQUIRE-
4 MENTS.—In order to be eligible for a multistate
5 grant under this subsection, each eligible entity that
6 comprises a multistate group shall—

7 “(A) submit to the Secretary a Cybersecu-
8 rity Plan for approval in accordance with sub-
9 section (i); and

10 “(B) establish a cybersecurity planning
11 committee under subsection (g).

12 “(3) APPLICATION.—

13 “(A) IN GENERAL.—A multistate group
14 applying for a multistate grant under para-
15 graph (1) shall submit to the Secretary an ap-
16 plication at such time, in such manner, and
17 containing such information as the Secretary
18 may require.

19 “(B) JOINT CYBERSECURITY PLAN.—An
20 application of a multistate group under sub-
21 paragraph (A) shall include a plan describing—

22 “(i) the division of responsibilities
23 among the eligible entities that comprise
24 the multistate group for administering the
25 grant for which application is being made;

1 “(ii) the distribution of funding from
2 such a grant among the eligible entities
3 that comprise the multistate group; and

4 “(iii) how the eligible entities that
5 comprise the multistate group will work to-
6 gether to implement the Cybersecurity
7 Plan of each of those eligible entities.

8 “(g) PLANNING COMMITTEES.—

9 “(1) IN GENERAL.—An eligible entity applying
10 for a grant under this section shall establish a cyber-
11 security planning committee to—

12 “(A) assist in the development, implemen-
13 tation, and revision of the Cybersecurity Plan of
14 the eligible entity;

15 “(B) approve the Cybersecurity Plan of the
16 eligible entity; and

17 “(C) assist in the determination of effec-
18 tive funding priorities for a grant under this
19 section in accordance with subsection (h).

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

22 “(A) be comprised of representatives from
23 the eligible entity and counties, cities, towns,
24 and Tribes within the jurisdiction of the eligible
25 entity; and

1 “(B) include, as appropriate, representa-
2 tives of rural, suburban, and high-population
3 jurisdictions.

4 “(3) CYBERSECURITY EXPERTISE.—Not less
5 than ½ of the representatives of a committee estab-
6 lished under paragraph (1) shall have professional
7 experience relating to cybersecurity or information
8 technology.

9 “(4) RULE OF CONSTRUCTION REGARDING EX-
10 ISTING PLANNING COMMITTEES.—Nothing in this
11 subsection may be construed to require an eligible
12 entity to establish a cybersecurity planning com-
13 mittee if the eligible entity has established and uses
14 a multijurisdictional planning committee or commis-
15 sion that meets the requirements of this subsection.

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

18 “(1) implement the Cybersecurity Plan of the
19 eligible entity;

20 “(2) develop or revise the Cybersecurity Plan of
21 the eligible entity; or

22 “(3) assist with activities that address immi-
23 nent cybersecurity risks or cybersecurity threats to
24 the information systems of the eligible entity or a

1 local or Tribal government within the jurisdiction of
2 the eligible entity.

3 “(i) APPROVAL OF PLANS.—

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

11 “(2) PLAN REQUIREMENTS.—In approving a
12 Cybersecurity Plan of an eligible entity under this
13 subsection, the Director shall ensure that the Cyber-
14 security Plan—

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

17 “(B) upon the issuance of the Homeland
18 Security Strategy to Improve the Cybersecurity
19 of State, Local, Tribal, and Territorial Govern-
20 ments authorized pursuant to section 2210(e),
21 complies, as appropriate, with the goals and ob-
22 jectives of the strategy; and

23 “(C) has been approved by the cybersecu-
24 rity planning committee of the eligible entity es-
25 tablished under subsection (g).

1 “(3) APPROVAL OF REVISIONS.—The Secretary,
2 acting through the Director, may approve revisions
3 to a Cybersecurity Plan as the Director determines
4 appropriate.

5 “(4) EXCEPTION.—Notwithstanding subsection
6 (e) and paragraph (1) of this subsection, the Sec-
7 retary may award a grant under this section to an
8 eligible entity that does not submit a Cybersecurity
9 Plan to the Secretary if—

10 “(A) the eligible entity certifies to the Sec-
11 retary that—

12 “(i) the activities that will be sup-
13 ported by the grant are integral to the de-
14 velopment of the Cybersecurity Plan of the
15 eligible entity; and

16 “(ii) the eligible entity will submit by
17 September 30, 2023, to the Secretary a
18 Cybersecurity Plan for review, and if ap-
19 propriate, approval; or

20 “(B) the eligible entity certifies to the Sec-
21 retary, and the Director confirms, that the eli-
22 gible entity will use funds from the grant to as-
23 sist with the activities described in subsection
24 (h)(3).

25 “(j) LIMITATIONS ON USES OF FUNDS.—

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

4 “(A) to supplant State, local, or Tribal
5 funds;

6 “(B) for any recipient cost-sharing con-
7 tribution;

8 “(C) to pay a demand for ransom in an at-
9 tempt to regain access to information or an in-
10 formation system of the eligible entity or of a
11 local or Tribal government within the jurisdic-
12 tion of the eligible entity;

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 of the eligible entity or of
17 a local or Tribal government within the jurisdic-
18 tion of the eligible entity.

19 “(2) PENALTIES.—In addition to any other
20 remedy available, the Secretary may take such ac-
21 tions as are necessary to ensure that a recipient of
22 a grant under this section uses the grant for the
23 purposes for which the grant is awarded.

24 “(k) OPPORTUNITY TO AMEND APPLICATIONS.—In
25 considering applications for grants under this section, the

1 Secretary shall provide applicants with a reasonable op-
2 portunity to correct defects, if any, in such applications
3 before making final awards.

4 “(1) APPORTIONMENT.—For fiscal year 2022 and
5 each fiscal year thereafter, the Secretary shall apportion
6 amounts appropriated to carry out this section among
7 States as follows:

8 “(1) BASELINE AMOUNT.—The Secretary shall
9 first apportion 0.25 percent of such amounts to each
10 of American Samoa, the Commonwealth of the
11 Northern Mariana Islands, Guam, the Virgin Is-
12 lands,, and 0.75 percent of such amounts to each of
13 the remaining States.

14 “(2) REMAINDER.—The Secretary shall appor-
15 tion the remainder of such amounts in the ratio
16 that—

17 “(A) the population of each eligible entity,
18 bears to

19 “(B) the population of all eligible entities.

20 “(m) FEDERAL SHARE.—

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

1 “(A) in the case of a grant to an eligible
2 entity—

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

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

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

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

7 and

8 “(v) for fiscal year 2026 and each
9 subsequent fiscal year, 50 percent; and

10 “(B) in the case of a grant to a multistate
11 group—

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

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

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

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

16 and

17 “(v) for fiscal year 2026 and each
18 subsequent fiscal year, 55 percent.

19 “(n) RESPONSIBILITIES OF GRANTEES.—

20 “(1) CERTIFICATION.—Each eligible entity or
21 multistate group that receives a grant under this
22 section shall certify to the Secretary that the grant
23 will be used—

24 “(A) for the purpose for which the grant
25 is awarded; and

1 “(B) in compliance with, as the case may
2 be—

3 “(i) the Cybersecurity Plan of the eli-
4 gible entity;

5 “(ii) the Cybersecurity Plans of the el-
6 igible entities that comprise the multistate
7 group; or

8 “(iii) a purpose approved by the Sec-
9 retary under subsection (h).

10 “(2) AVAILABILITY OF FUNDS TO LOCAL AND
11 TRIBAL GOVERNMENTS.—Not later than 45 days
12 after the date on which an eligible entity or
13 multistate group receives a grant under this section,
14 the eligible entity or multistate group shall, without
15 imposing unreasonable or unduly burdensome re-
16 quirements as a condition of receipt, obligate or oth-
17 erwise make available to local and Tribal govern-
18 ments within the jurisdiction of the eligible entity or
19 the eligible entities that comprise the multistate
20 group, consistent with the Cybersecurity Plan of the
21 eligible entity or the Cybersecurity Plans of the eligi-
22 ble entities that comprise the multistate group—

23 “(A) not less than 80 percent of funds
24 available under the grant;

1 “(B) with the consent of the local and
2 Tribal governments, items, services, capabilities,
3 or activities having a value of not less than 80
4 percent of the amount of the grant; or

5 “(C) with the consent of the local and
6 Tribal governments, grant funds combined with
7 other items, services, capabilities, or activities
8 having the total value of not less than 80 per-
9 cent of the amount of the grant.

10 “(3) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL AND TRIBAL GOVERNMENTS.—An eligible entity or multistate group shall certify to the Secretary that the eligible entity or multistate group has made the distribution to local, Tribal, and territorial governments required under paragraph (2).

17 “(4) EXTENSION OF PERIOD.—

18 “(A) IN GENERAL.—An eligible entity or
19 multistate group may request in writing that
20 the Secretary extend the period of time speci-
21 fied in paragraph (2) for an additional period
22 of time.

23 “(B) APPROVAL.—The Secretary may ap-
24 prove a request for an extension under subpara-
25 graph (A) if the Secretary determines the ex-

1 tension is necessary to ensure that the obliga-
2 tion and expenditure of grant funds align with
3 the purpose of the State and Local Cybersecu-
4 rity Grant Program.

5 “(5) EXCEPTION.—Paragraph (2) shall not
6 apply to the District of Columbia, the Common-
7 wealth of Puerto Rico, American Samoa, the Com-
8 monwealth of the Northern Mariana Islands, Guam,
9 the Virgin Islands, or a Federally recognized Indian
10 Tribe.

11 “(6) DIRECT FUNDING.—If an eligible entity
12 does not make a distribution to a local or Tribal
13 government required in accordance with paragraph
14 (2), the local or Tribal government may petition the
15 Secretary.

16 “(7) PENALTIES.—In addition to other rem-
17 edies available to the Secretary, the Secretary may
18 terminate or reduce the amount of a grant awarded
19 under this section to an eligible entity or transfer
20 grant funds previously awarded to such eligible enti-
21 ty directly to the appropriate local or Tribal govern-
22 ment if such eligible entity violates a requirement of
23 this subsection.

24 “(o) ADVISORY COMMITTEE.—

1 “(1) ESTABLISHMENT.—Not later than 120
2 days after the date of enactment of this section, the
3 Director shall establish a State and Local Cyberse-
4 curity Resiliency Committee to provide State, local,
5 and Tribal stakeholder expertise, situational aware-
6 ness, and recommendations to the Director, as ap-
7 propriate, regarding how to—

8 “(A) address cybersecurity risks and cyber-
9 security threats to information systems of
10 State, local, or Tribal governments; and

11 “(B) improve the ability of State, local,
12 and Tribal governments to prevent, protect
13 against, respond to, mitigate, and recover from
14 such cybersecurity risks and cybersecurity
15 threats.

16 “(2) DUTIES.—The committee established
17 under paragraph (1) shall—

18 “(A) submit to the Director recommenda-
19 tions that may inform guidance for applicants
20 for grants under this section;

21 “(B) upon the request of the Director, pro-
22 vide to the Director technical assistance to in-
23 form the review of Cybersecurity Plans sub-
24 mitted by applicants for grants under this sec-
25 tion, and, as appropriate, submit to the Direc-

1 tor recommendations to improve those plans
2 prior to the approval of the plans under sub-
3 section (i);

4 “(C) advise and provide to the Director
5 input regarding the Homeland Security Strat-
6 egy to Improve Cybersecurity for State, Local,
7 Tribal, and Territorial Governments required
8 under section 2210; and

9 “(D) upon the request of the Director, pro-
10 vide to the Director recommendations, as ap-
11 propriate, regarding how to—

12 “(i) address cybersecurity risks and
13 cybersecurity threats on information sys-
14 tems of State, local, or Tribal govern-
15 ments; and

16 “(ii) improve the cybersecurity resil-
17 ience of State, local, or Tribal govern-
18 ments.

19 “(3) MEMBERSHIP.—

20 “(A) NUMBER AND APPOINTMENT.—The
21 State and Local Cybersecurity Resiliency Com-
22 mittee established pursuant to paragraph (1)
23 shall be composed of 15 members appointed by
24 the Director, as follows:

1 “(i) Two individuals recommended to
2 the Director by the National Governors As-
3 sociation.

4 “(ii) Two individuals recommended to
5 the Director by the National Association of
6 State Chief Information Officers.

7 “(iii) One individual recommended to
8 the Director by the National Guard Bu-
9 reau.

10 “(iv) Two individuals recommended to
11 the Director by the National Association of
12 Counties.

13 “(v) One individual recommended to
14 the Director by the National League of
15 Cities.

16 “(vi) One individual recommended to
17 the Director by the United States Con-
18 ference of Mayors.

19 “(vii) One individual recommended to
20 the Director by the Multi-State Informa-
21 tion Sharing and Analysis Center.

22 “(viii) One individual recommended to
23 the Director by the National Congress of
24 American Indians.

1 “(viii) Four individuals who have edu-
2 cational and professional experience relat-
3 ing to cybersecurity work or cybersecurity
4 policy.

5 “(B) TERMS.—

6 “(i) IN GENERAL.—Subject to clause
7 (ii), each member of the State and Local
8 Cybersecurity Resiliency Committee shall
9 be appointed for a term of two years.

10 “(ii) EXCEPTION.—A term of a mem-
11 ber of the State and Local Cybersecurity
12 Resiliency Committee shall be three years
13 if the member is appointed initially to the
14 Committee upon the establishment of the
15 Committee.

16 “(iii) TERM REMAINDERS.—Any mem-
17 ber of the State and Local Cybersecurity
18 Resiliency Committee appointed to fill a
19 vacancy occurring before the expiration of
20 the term for which the member’s prede-
21 cessor was appointed shall be appointed
22 only for the remainder of such term. A
23 member may serve after the expiration of
24 such member’s term until a successor has
25 taken office.

1 “(iv) VACANCIES.—A vacancy in State
2 and Local Cybersecurity Resiliency Com-
3 mittee shall be filled in the manner in
4 which the original appointment was made.

5 “(C) PAY.—Members of the State and
6 Local Cybersecurity Resiliency Committee shall
7 serve without pay.

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

12 “(5) PERMANENT AUTHORITY.—Notwith-
13 standing section 14 of the Federal Advisory Com-
14 mittee Act (5 U.S.C. App.), the State and Local Cy-
15 bersecurity Resiliency Committee shall be a perma-
16 nent authority.

17 “(p) REPORTS.—

18 “(1) ANNUAL REPORTS BY GRANT RECIPI-
19 ENTS.—

20 “(A) IN GENERAL.—Not later than 30
21 days after the end of a fiscal year during which
22 an eligible entity or multistate group receives
23 funds under this section, the eligible entity or
24 multistate group shall submit to the Secretary
25 a report on the progress of the eligible entity or

1 multistate group in implementing the Cyberse-
2 curity Plan of the eligible entity or Cybersecu-
3 rity Plans of the eligible entities that comprise
4 the multistate group, as the case may be.

5 “(B) ABSENCE OF PLAN.—Not later than
6 30 days after the end of a fiscal year during
7 which an eligible entity that does not have a
8 Cybersecurity Plan receives funds under this
9 section, the eligible entity shall submit to the
10 Secretary a report describing how the eligible
11 entity obligated and expended grant funds dur-
12 ing the fiscal year to—

13 “(i) develop a Cybersecurity Plan; or

14 “(ii) assist with the activities de-
15 scribed in subsection (h)(3).

16 “(C) PUBLIC AVAILABILITY.—The Sec-
17 retary, acting through the Director, shall make
18 each report submitted under subparagraphs (A)
19 and (B) publicly available, including by making
20 each such report available on the internet
21 website of the Agency, subject to any redactions
22 the Director determines necessary to protect
23 classified or other sensitive information.

24 “(2) ANNUAL REPORTS TO CONGRESS.—Not
25 less than frequently than once per year, the Sec-

1 retary, acting through the Director, shall submit to
2 Congress a report on the use of grants awarded
3 under this section and any progress made toward
4 the following:

5 “(A) Achieving the objectives set forth in
6 the Homeland Security Strategy to Improve the
7 Cybersecurity of State, Local, Tribal, and Ter-
8 ritorial Governments, upon the date on which
9 the strategy is issued under section 2210.

10 “(B) Developing, implementing, or revising
11 Cybersecurity Plans.

12 “(C) Reducing cybersecurity risks and cy-
13 bersecurity threats to information systems
14 owned or operated by State, local, and Tribal
15 governments as a result of the award of such
16 grants.

17 “(q) AUTHORIZATION OF APPROPRIATIONS.—There
18 are authorized to be appropriated for grants under this
19 section—

20 “(1) for each of fiscal years 2022 through
21 2026, \$500,000,000; and

22 “(2) for each subsequent fiscal year, such sums
23 as may be necessary.

1 **“SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOP-**
2 **MENT FOR STATE, LOCAL, TRIBAL, AND TER-**
3 **RITORIAL GOVERNMENT OFFICIALS.**

4 “The Secretary, acting through the Director, shall
5 develop, regularly update, and maintain a resource guide
6 for use by State, local, Tribal, and territorial government
7 officials, including law enforcement officers, to help such
8 officials identify, prepare for, detect, protect against, re-
9 spond to, and recover from cybersecurity risks (as such
10 term is defined in section 2209), cybersecurity threats,
11 and incidents (as such term is defined in section 2209).”.

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

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

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

17 **SEC. 3. STRATEGY.**

18 (a) HOMELAND SECURITY STRATEGY TO IMPROVE
19 THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND
20 TERRITORIAL GOVERNMENTS.—Section 2210 of the
21 Homeland Security Act of 2002 (6 U.S.C. 660) is amend-
22 ed by adding at the end the following new subsection:

1 “(e) HOMELAND SECURITY STRATEGY TO IMPROVE
2 THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND
3 TERRITORIAL GOVERNMENTS.—

4 “(1) IN GENERAL.—

5 “(A) REQUIREMENT.—Not later than 270
6 days after the date of the enactment of this
7 subsection, the Secretary, acting through the
8 Director, shall, in coordination with the heads
9 of appropriate Federal agencies, State, local,
10 Tribal, and territorial governments, the State
11 and Local Cybersecurity Resilience Committee
12 established under section 2220A, and other
13 stakeholders, as appropriate, develop and make
14 publicly available a Homeland Security Strategy
15 to Improve the Cybersecurity of State, Local,
16 Tribal, and Territorial Governments.

17 “(B) RECOMMENDATIONS AND REQUIRE-
18 MENTS.—The strategy required under subpara-
19 graph (A) shall—

20 “(i) provide recommendations relating
21 to the ways in which the Federal Govern-
22 ment should support and promote the abil-
23 ity of State, local, Tribal, and territorial
24 governments to identify, protect against,
25 detect, respond to, and recover from cyber-

1 security risks (as such term is defined in
2 section 2209), cybersecurity threats, and
3 incidents (as such term is defined in sec-
4 tion 2209); and

5 “(ii) establish baseline requirements
6 for cybersecurity plans under this section
7 and principles with which such plans shall
8 align.

9 “(2) CONTENTS.—The strategy required under
10 paragraph (1) shall—

11 “(A) identify capability gaps in the ability
12 of State, local, Tribal, and territorial govern-
13 ments to identify, protect against, detect, re-
14 spond to, and recover from cybersecurity risks,
15 cybersecurity threats, and incidents;

16 “(B) identify Federal resources and capa-
17 bilities that are available or could be made
18 available to State, local, Tribal, and territorial
19 governments to help those governments identify,
20 protect against, detect, respond to, and recover
21 from cybersecurity risks, cybersecurity threats,
22 and incidents;

23 “(C) identify and assess the limitations of
24 Federal resources and capabilities available to
25 State, local, Tribal, and territorial governments

1 to help those governments identify, protect
2 against, detect, respond to, and recover from
3 cybersecurity risks, cybersecurity threats, and
4 incidents, and make recommendations to ad-
5 dress such limitations;

6 “(D) identify opportunities to improve the
7 coordination of the Agency with Federal and
8 non-Federal entities, such as the Multi-State
9 Information Sharing and Analysis Center, to
10 improve—

11 “(i) incident exercises, information
12 sharing and incident notification proce-
13 dures;

14 “(ii) the ability for State, local, Trib-
15 al, and territorial governments to volun-
16 tarily adapt and implement guidance in
17 Federal binding operational directives; and

18 “(iii) opportunities to leverage Federal
19 schedules for cybersecurity investments
20 under section 502 of title 40, United
21 States Code;

22 “(E) recommend new initiatives the Fed-
23 eral Government should undertake to improve
24 the ability of State, local, Tribal, and territorial
25 governments to identify, protect against, detect,

1 respond to, and recover from cybersecurity
2 risks, cybersecurity threats, and incidents;

3 “(F) set short-term and long-term goals
4 that will improve the ability of State, local,
5 Tribal, and territorial governments to identify,
6 protect against, detect, respond to, and recover
7 from cybersecurity risks, cybersecurity threats,
8 and incidents; and

9 “(G) set dates, including interim bench-
10 marks, as appropriate for State, local, Tribal,
11 and territorial governments to establish baseline
12 capabilities to identify, protect against, detect,
13 respond to, and recover from cybersecurity
14 risks, cybersecurity threats, and incidents.

15 “(3) CONSIDERATIONS.—In developing the
16 strategy required under paragraph (1), the Director,
17 in coordination with the heads of appropriate Fed-
18 eral agencies, State, local, Tribal, and territorial
19 governments, the State and Local Cybersecurity Re-
20 silience Committee established under section 2220A,
21 and other stakeholders, as appropriate, shall con-
22 sider—

23 “(A) lessons learned from incidents that
24 have affected State, local, Tribal, and territorial

1 governments, and exercises with Federal and
2 non-Federal entities;

3 “(B) the impact of incidents that have af-
4 fected State, local, Tribal, and territorial gov-
5 ernments, including the resulting costs to such
6 governments;

7 “(C) the information related to the interest
8 and ability of state and non-state threat actors
9 to compromise information systems (as such
10 term is defined in section 102 of the Cybersecu-
11 rity Act of 2015 (6 U.S.C. 1501)) owned or op-
12 erated by State, local, Tribal, and territorial
13 governments;

14 “(D) emerging cybersecurity risks and cy-
15 bersecurity threats to State, local, Tribal, and
16 territorial governments resulting from the de-
17 ployment of new technologies; and

18 “(E) recommendations made by the State
19 and Local Cybersecurity Resilience Committee
20 established under section 2220A.”.

21 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE
22 CYBERSECURITY AND INFRASTRUCTURE SECURITY AGEN-
23 CY.—Section 2202(c) of the Homeland Security Act of
24 2002 (6 U.S.C. 652(c)) is amended—

1 (1) by redesignating paragraphs (6), (7), (8),
2 (9), (10), and (11) as paragraphs (10), (11), (12),
3 (13), (14), and (15), respectively; and

4 (2) by inserting after paragraph (5) the fol-
5 lowing new paragraphs:

6 “(6) develop program guidance, in consultation
7 with the State and Local Government Cybersecurity
8 Resiliency Committee established under section
9 2220A, for the State and Local Cybersecurity Grant
10 Program under such section or any other homeland
11 security assistance administered by the Department
12 to improve cybersecurity;

13 “(7) review, in consultation with the State and
14 Local Cybersecurity Resiliency Committee, all cyber-
15 security plans of State, local, Tribal, and territorial
16 governments developed pursuant to any homeland
17 security assistance administered by the Department
18 to improve cybersecurity;

19 “(8) provide expertise and technical assistance
20 to State, local, Tribal, and territorial government of-
21 ficials with respect to cybersecurity;

22 “(9) provide education, training, and capacity
23 development to enhance the security and resilience
24 of cybersecurity and infrastructure security;”.

1 (c) FEASIBILITY STUDY.—Not later than 180 days
2 after the date of the enactment of this Act, the Director
3 of the Cybersecurity and Infrastructure Security of the
4 Department of Homeland Security shall conduct a study
5 to assess the feasibility of implementing a short-term rota-
6 tional program for the detail to the Agency of approved
7 State, local, Tribal, and territorial government employees
8 in cyber workforce positions.

9 **SEC. 4. TITLE XXII TECHNICAL AND CLERICAL AMEND-**
10 **MENTS.**

11 (a) TECHNICAL AMENDMENTS.—

12 (1) HOMELAND SECURITY ACT OF 2002.—Sub-
13 title A of title XXII of the Homeland Security Act
14 of 2002 (6 U.S.C. 651 et seq.) is amended—

15 (A) in the first section 2215 (6 U.S.C.
16 665; relating to the duties and authorities relat-
17 ing to .gov internet domain), by amending the
18 section enumerator and heading to read as fol-
19 lows:

20 **“SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV**
21 **INTERNET DOMAIN.”;**

22 (B) in the second section 2215 (6 U.S.C.
23 665b; relating to the joint cyber planning of-
24 fice), by amending the section enumerator and
25 heading to read as follows:

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

2 (C) in the third section 2215 (6 U.S.C.
3 665c; relating to the Cybersecurity State Coor-
4 dinator), by amending the section enumerator
5 and heading to read as follows:

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

7 (D) in the fourth section 2215 (6 U.S.C.
8 665d; relating to Sector Risk Management
9 Agencies), by amending the section enumerator
10 and heading to read as follows:

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

12 (E) in section 2216 (6 U.S.C. 665e; relat-
13 ing to the Cybersecurity Advisory Committee),
14 by amending the section enumerator and head-
15 ing to read as follows:

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

17 (F) in section 2217 (6 U.S.C. 665f; relat-
18 ing to Cybersecurity Education and Training
19 Programs), by amending the section enu-
20 merator and heading to read as follows:

21 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING**
22 **PROGRAMS.”.**

23 (2) CONSOLIDATED APPROPRIATIONS ACT,
24 2021.—Paragraph (1) of section 904(b) of division U
25 of the Consolidated Appropriations Act, 2021 (Pub-
26 lic Law 116–260) is amended, in the matter pre-

1 ceding subparagraph (A), by inserting “of 2002”
2 after “Homeland Security Act”.

3 (b) CLERICAL AMENDMENT.—The table of contents
4 in section 1(b) of the Homeland Security Act of 2002 is
5 amended by striking the items relating to sections 2214
6 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.”.