

117TH CONGRESS  
1ST SESSION

# H. R. 3138

---

IN THE SENATE OF THE UNITED STATES

JULY 21, 2021

Received; read twice and referred to the Committee on Homeland Security and  
Governmental Affairs

---

## AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “State and Local Cyber-  
3 security Improvement Act”.

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

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

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

12 “(a) DEFINITIONS.—In this section:

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

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

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

22 “(A) a State; or

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

1 start of any fiscal year in which a grant under  
2 this section is awarded—

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

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

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

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

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

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

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

1 website, email, virtual private network, or custom  
2 application.

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  
10 the information system’s owner, operator, or another  
11 person.

12 “(10) STATE AND LOCAL CYBERSECURITY  
13 GRANT PROGRAM.—The term ‘State and Local Cy-  
14 bersecurity Grant Program’ means the program es-  
15 tablished under subsection (b).

16 “(11) STATE AND LOCAL CYBERSECURITY RE-  
17 SILIENCE COMMITTEE.—The term ‘State and Local  
18 Cybersecurity 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  
23 be 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  
2 Tribal organizations.

3 “(2) APPLICATION.—An eligible entity seeking  
4 a grant under the State and Local Cybersecurity  
5 Grant Program shall submit to the Secretary an ap-  
6 plication at such time, in such manner, and con-  
7 taining such information as the Secretary may re-  
8 quire.

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

12 “(1)(A) the Cybersecurity Plan of the eligible  
13 entity or the Cybersecurity Plans of the eligible enti-  
14 ties that comprise the multistate group; and

15 “(B) the Homeland Security Strategy to Im-  
16 prove the Cybersecurity of State, Local, Tribal, and  
17 Territorial Governments developed under section  
18 2210(e)(1); or

19 “(2) activities carried out under paragraphs  
20 (3), (4), and (5) of subsection (h).

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

25 “(e) CYBERSECURITY PLANS.—

1           “(1) IN GENERAL.—An eligible entity applying  
2 for a grant under this section shall submit to the  
3 Secretary 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 pro-  
8 tect against cybersecurity risks and cybersecu-  
9 rity threats to information systems of State,  
10 local, or Tribal organizations;

11                   “(B) describe, to the extent practicable,  
12 how 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  
16 of the eligible entity or by local or Tribal  
17 organizations within the jurisdiction of the  
18 eligible entity and the information tech-  
19 nology deployed on those information sys-  
20 tems, including legacy information systems  
21 and information technology that are no  
22 longer supported by the manufacturer of  
23 the systems 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  
3 or Tribal organizations within the jurisdic-  
4 tion of the eligible entity and between  
5 those information systems and information  
6 systems not owned or operated by the eligi-  
7 ble entity or by local or Tribal organiza-  
8 tions within the jurisdiction of the eligible  
9 entity;

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

17 “(iv) implement a process of contin-  
18 uous cybersecurity vulnerability assess-  
19 ments and threat mitigation practices  
20 prioritized by degree of risk to address cy-  
21 bersecurity risks and cybersecurity threats  
22 on information systems of the eligible enti-  
23 ty or local or Tribal organizations;

24 “(v) ensure that State, local, and  
25 Tribal organizations that own or operate

1 information systems that are located with-  
2 in the jurisdiction of the eligible entity—

3 “(I) adopt best practices and  
4 methodologies to enhance cybersecu-  
5 rity, such as the practices set forth in  
6 the cybersecurity framework developed  
7 by, and the cyber supply chain risk  
8 management best practices identified  
9 by, the National Institute of Stand-  
10 ards 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 cybersecu-  
22 rity 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  
4           National Institute of Standards and Tech-  
5           nology to identify and mitigate any gaps in  
6           the cybersecurity workforces of State,  
7           local, or Tribal organizations, enhance re-  
8           cruitment and retention efforts for such  
9           workforces, and bolster the knowledge,  
10          skills, and abilities of State, local, and  
11          Tribal organization personnel to address  
12          cybersecurity risks and cybersecurity  
13          threats, such as through cybersecurity hy-  
14          giene training;

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

24          “(x) assess and mitigate, to the great-  
25          est degree possible, cybersecurity risks and

1           cybersecurity threats related to critical in-  
2           frastructure and key resources, the deg-  
3           radation of which may impact the perform-  
4           ance of information systems within the ju-  
5           risdiction of the eligible entity;

6           “(xi) enhance capabilities to share  
7           cyber threat indicators and related infor-  
8           mation between the eligible entity and local  
9           and Tribal organizations that own or oper-  
10          ate information systems within the juris-  
11          diction of the eligible entity, including by  
12          expanding existing information sharing  
13          agreements with the Department;

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

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

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

1                   “(I) local and Tribal organiza-  
2                   tions within the jurisdiction of the eli-  
3                   gible 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; and

13                  “(xv) implement an information tech-  
14                  nology and operational technology mod-  
15                  ernization cybersecurity review process  
16                  that ensures alignment between informa-  
17                  tion technology and operational technology  
18                  cybersecurity objectives;

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

1           “(D) outline, to the extent practicable, the  
2           necessary resources and a timeline for imple-  
3           menting the plan; and

4           “(E) describe how the eligible entity will  
5           measure progress towards implementing the  
6           plan.

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

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

15           “(B) programs provided by the eligible en-  
16           tity to support local and Tribal organizations  
17           and owners and operators of critical infrastruc-  
18           ture to address cybersecurity risks and cyberse-  
19           curity threats.

20           “(4) MANAGEMENT OF FUNDS.—An eligible en-  
21           tity applying for a grant under this section shall  
22           agree to designate the Chief Information Officer, the  
23           Chief Information Security Officer, or an equivalent  
24           official of the eligible entity as the primary official

1 for the management and allocation of funds awarded  
2 under this section.

3 “(f) MULTISTATE GRANTS.—

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

10 “(2) SATISFACTION OF OTHER REQUIRE-  
11 MENTS.—In order to be eligible for a multistate  
12 grant under this subsection, each eligible entity that  
13 comprises a multistate group shall submit to the  
14 Secretary—

15 “(A) a Cybersecurity Plan for approval in  
16 accordance with subsection (i); and

17 “(B) a plan for establishing a cybersecu-  
18 rity planning committee under subsection (g).

19 “(3) APPLICATION.—

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

1           “(B) MULTISTATE PROJECT DESCRIP-  
2           TION.—An application of a multistate group  
3           under subparagraph (A) shall include a plan de-  
4           scribing—

5                   “(i) the division of responsibilities  
6                   among the eligible entities that comprise  
7                   the multistate group for administering the  
8                   grant for which application is being made;

9                   “(ii) the distribution of funding from  
10                  such a grant among the eligible entities  
11                  that comprise the multistate group; and

12                  “(iii) how the eligible entities that  
13                  comprise the multistate group will work to-  
14                  gether to implement the Cybersecurity  
15                  Plan of each of those eligible entities.

16           “(g) PLANNING COMMITTEES.—

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

20                           “(A) assist in the development, implemen-  
21                           tation, and revision of the Cybersecurity Plan of  
22                           the eligible entity;

23                           “(B) approve the Cybersecurity Plan of the  
24                           eligible entity; and

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

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

5           “(A) be comprised of representatives from  
6           the eligible entity and counties, cities, towns,  
7           Tribes, and public educational and health institutions within the jurisdiction of the eligible entity; and  
8           “(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.  
9           “(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.  
10           “(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

11           “(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.  
12           “(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.  
13           “(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

14           “(3) CYBERSECURITY EXPERTISE.—Not less  
15           than ½ of the representatives of a committee established under paragraph (1) shall have professional  
16           experience relating to cybersecurity or information  
17           technology.  
18           “(3) CYBERSECURITY EXPERTISE.—Not less than ½ of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

19           “(4) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMITTEES.—Nothing in this  
20           subsection may be construed to require an eligible  
21           entity to establish a cybersecurity planning committee if the eligible entity has established and uses  
22           a multijurisdictional planning committee or commis-  
23           a multijurisdictional planning committee or commis-  
24           a multijurisdictional planning committee or commis-

1 sion that meets, or may be leveraged to meet, the re-  
2 quirements of this subsection.

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

5 “(1) implement the Cybersecurity Plan of the  
6 eligible entity;

7 “(2) develop or revise the Cybersecurity Plan of  
8 the eligible entity; or

9 “(3) assist with activities that address immi-  
10 nent cybersecurity risks or cybersecurity threats to  
11 the information systems of the eligible entity or a  
12 local or Tribal organization within the jurisdiction of  
13 the eligible entity.

14 “(i) APPROVAL OF PLANS.—

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

22 “(2) PLAN REQUIREMENTS.—In approving a  
23 Cybersecurity Plan of an eligible entity under this  
24 subsection, the Director shall ensure that the Cyber-  
25 security Plan—



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

3           “(B) upon the issuance of the Homeland  
4           Security Strategy to Improve the Cybersecurity  
5           of State, Local, Tribal, and Territorial Govern-  
6           ments authorized pursuant to section 2210(e),  
7           complies, as appropriate, with the goals and ob-  
8           jectives of the strategy; and

9           “(C) has been approved by the cybersecu-  
10          rity planning committee of the eligible entity es-  
11          tablished under subsection (g).

12          “(3) APPROVAL OF REVISIONS.—The Secretary,  
13          acting through the Director, may approve revisions  
14          to a Cybersecurity Plan as the Director determines  
15          appropriate.

16          “(4) EXCEPTION.—Notwithstanding subsection  
17          (e) and paragraph (1) of this subsection, the Sec-  
18          retary may award a grant under this section to an  
19          eligible entity that does not submit a Cybersecurity  
20          Plan to the Secretary if—

21                 “(A) the eligible entity certifies to the Sec-  
22                 retary that—

23                         “(i) the activities that will be sup-  
24                         ported by the grant are integral to the de-

1           velopment of the Cybersecurity Plan of the  
2           eligible entity; and

3                   “(ii) the eligible entity will submit by  
4           September 30, 2023, to the Secretary a  
5           Cybersecurity Plan for review, and if ap-  
6           propriate, approval; or

7                   “(B) the eligible entity certifies to the Sec-  
8           retary, and the Director confirms, that the eli-  
9           gible entity will use funds from the grant to as-  
10          sist with the activities described in subsection  
11          (h)(3).

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

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

16                   “(A) to supplant State, local, or Tribal  
17          funds;

18                   “(B) for any recipient cost-sharing con-  
19          tribution;

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

22                   “(i) regain access to information or  
23          an information system of the eligible entity  
24          or of a local or Tribal organization within  
25          the jurisdiction of the eligible entity; or

1           “(ii) prevent the disclosure of infor-  
2           mation that has been removed without au-  
3           thorization from an information system of  
4           the eligible entity or of a local or Tribal or-  
5           ganization within the jurisdiction of the eli-  
6           gible entity;

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

8           “(E) for any purpose that does not address  
9           cybersecurity risks or cybersecurity threats on  
10          information systems of the eligible entity or of  
11          a local or Tribal organization within the juris-  
12          diction of the eligible entity.

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

18          “(3) RULE OF CONSTRUCTION.—Nothing in  
19          paragraph (1) may be construed to prohibit the use  
20          of grant funds provided to a State, local, or Tribal  
21          organization for otherwise permissible uses under  
22          this section on the basis that a State, local, or Trib-  
23          al organization has previously used State, local, or  
24          Tribal funds to support the same or similar uses.

1       “(k) OPPORTUNITY TO AMEND APPLICATIONS.—In  
2 considering applications for grants under this section, the  
3 Secretary shall provide applicants with a reasonable op-  
4 portunity to correct defects, if any, in such applications  
5 before making final awards.

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

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

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

19                   “(A) the population of each eligible entity,  
20 bears to

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

22           “(3) MINIMUM ALLOCATION TO INDIAN  
23 TRIBES.—

24                   “(A) IN GENERAL.—In apportioning  
25 amounts under this section, the Secretary shall

1 ensure that, for each fiscal year, directly eligible  
2 Tribes collectively receive, from amounts appro-  
3 priated under the State and Local Cybersecu-  
4 rity Grant Program, not less than an amount  
5 equal to three percent of the total amount ap-  
6 propriated for grants under this section.

7 “(B) ALLOCATION.—Of the amount re-  
8 served under subparagraph (A), funds shall be  
9 allocated in a manner determined by the Sec-  
10 retary in consultation with Indian tribes.

11 “(C) EXCEPTION.—This paragraph shall  
12 not apply in any fiscal year in which the Sec-  
13 retary—

14 “(i) receives fewer than five applica-  
15 tions from Indian tribes; or

16 “(ii) does not approve at least two ap-  
17 plications from Indian tribes.

18 “(m) FEDERAL SHARE.—

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

23 “(A) in the case of a grant to an eligible  
24 entity—

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

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

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

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

4 and

5 “(v) for fiscal year 2026 and each  
6 subsequent fiscal year, 50 percent; and

7 “(B) in the case of a grant to a multistate  
8 group—

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

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

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

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

13 and

14 “(v) for fiscal year 2026 and each  
15 subsequent fiscal year, 55 percent.

16 “(2) WAIVER.—The Secretary may waive or  
17 modify the requirements of paragraph (1) for an In-  
18 dian tribe if the Secretary determines such a waiver  
19 is in the public interest.

20 “(n) RESPONSIBILITIES OF GRANTEES.—

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

1           “(A) for the purpose for which the grant  
2           is awarded; and

3           “(B) in compliance with, as the case may  
4           be—

5                   “(i) the Cybersecurity Plan of the eli-  
6                   gible entity;

7                   “(ii) the Cybersecurity Plans of the eli-  
8                   gible entities that comprise the multistate  
9                   group; or

10                   “(iii) a purpose approved by the Sec-  
11                   retary under subsection (h) or pursuant to  
12                   an exception under subsection (i).

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

1 rity Plans of the eligible entities that comprise the  
2 multistate group—

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

5 “(B) with the consent of the local and  
6 Tribal organizations, items, services, capabili-  
7 ties, or activities having a value of not less than  
8 80 percent of the amount of the grant; or

9 “(C) with the consent of the local and  
10 Tribal organizations, grant funds combined  
11 with other items, services, capabilities, or activi-  
12 ties having the total value of not less than 80  
13 percent of the amount of the grant.

14 “(3) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL AND TRIBAL OR-  
15 GANIZATIONS.—An eligible entity or multistate  
16 group shall certify to the Secretary that the eligible  
17 entity or multistate group has made the distribution  
18 to local, Tribal, and territorial governments required  
19 under paragraph (2).

21 “(4) EXTENSION OF PERIOD.—

22 “(A) IN GENERAL.—An eligible entity or  
23 multistate group may request in writing that  
24 the Secretary extend the period of time speci-



1           fied in paragraph (2) for an additional period  
2           of time.

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

10          “(5) EXCEPTION.—Paragraph (2) shall not  
11          apply to the District of Columbia, the Common-  
12          wealth of Puerto Rico, American Samoa, the Com-  
13          monwealth of the Northern Mariana Islands, Guam,  
14          the Virgin Islands, or an Indian tribe.

15          “(6) DIRECT FUNDING.—If an eligible entity  
16          does not make a distribution to a local or Tribal or-  
17          ganization required in accordance with paragraph  
18          (2), the local or Tribal organization may petition the  
19          Secretary to request that grant funds be provided di-  
20          rectly to the local or Tribal organization.

21          “(7) PENALTIES.—In addition to other rem-  
22          edies available to the Secretary, the Secretary may  
23          terminate or reduce the amount of a grant awarded  
24          under this section to an eligible entity or distribute  
25          grant funds previously awarded to such eligible enti-

1 ty directly to the appropriate local or Tribal organi-  
2 zation as a replacement grant in an amount the Sec-  
3 retary determines appropriate if such eligible entity  
4 violates a requirement of this subsection.

5 “(o) ADVISORY COMMITTEE.—

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

13 “(A) address cybersecurity risks and cyber-  
14 security threats to information systems of  
15 State, local, or Tribal organizations; and

16 “(B) improve the ability of State, local,  
17 and Tribal organizations to prevent, protect  
18 against, respond to, mitigate, and recover from  
19 such cybersecurity risks and cybersecurity  
20 threats.

21 “(2) DUTIES.—The committee established  
22 under paragraph (1) shall—

23 “(A) submit to the Director recommenda-  
24 tions that may inform guidance for applicants  
25 for grants under this section;

1           “(B) upon the request of the Director, pro-  
2           vide to the Director technical assistance to in-  
3           form the review of Cybersecurity Plans sub-  
4           mitted by applicants for grants under this sec-  
5           tion, and, as appropriate, submit to the Direc-  
6           tor recommendations to improve those plans  
7           prior to the approval of the plans under sub-  
8           section (i);

9           “(C) advise and provide to the Director  
10          input regarding the Homeland Security Strat-  
11          egy to Improve Cybersecurity for State, Local,  
12          Tribal, and Territorial Governments required  
13          under section 2210;

14          “(D) upon the request of the Director, pro-  
15          vide to the Director recommendations, as ap-  
16          propriate, regarding how to—

17                 “(i) address cybersecurity risks and  
18                 cybersecurity threats on information sys-  
19                 tems of State, local, or Tribal organiza-  
20                 tions; and

21                 “(ii) improve the cybersecurity resil-  
22                 ience of State, local, or Tribal organiza-  
23                 tions; and

24          “(E) regularly coordinate with the State,  
25          Local, Tribal and Territorial Government Co-

1           ordinating Council, within the Critical Infra-  
2           structure Partnership Advisory Council, estab-  
3           lished under section 871.

4           “(3) MEMBERSHIP.—

5                   “(A) NUMBER AND APPOINTMENT.—The  
6           State and Local Cybersecurity Resilience Com-  
7           mittee established pursuant to paragraph (1)  
8           shall be composed of 15 members appointed by  
9           the Director, as follows:

10                   “(i) Two individuals recommended to  
11           the Director by the National Governors As-  
12           sociation.

13                   “(ii) Two individuals recommended to  
14           the Director by the National Association of  
15           State Chief Information Officers.

16                   “(iii) One individual recommended to  
17           the Director by the National Guard Bu-  
18           reau.

19                   “(iv) Two individuals recommended to  
20           the Director by the National Association of  
21           Counties.

22                   “(v) One individual recommended to  
23           the Director by the National League of  
24           Cities.

1           “(vi) One individual recommended to  
2           the Director by the United States Con-  
3           ference of Mayors.

4           “(vii) One individual recommended to  
5           the Director by the Multi-State Informa-  
6           tion Sharing and Analysis Center.

7           “(viii) One individual recommended to  
8           the Director by the National Congress of  
9           American Indians.

10           “(viii) Four individuals who have edu-  
11           cational and professional experience relat-  
12           ing to cybersecurity work or cybersecurity  
13           policy.

14           “(B) TERMS.—

15           “(i) IN GENERAL.—Subject to clause  
16           (ii), each member of the State and Local  
17           Cybersecurity Resilience Committee shall  
18           be appointed for a term of two years.

19           “(ii) REQUIREMENT.—At least two  
20           members of the State and Local Cyberse-  
21           curity Resilience Committee shall also be  
22           members of the State, Local, Tribal and  
23           Territorial Government Coordinating  
24           Council, within the Critical Infrastructure

1 Partnership Advisory Council, established  
2 under section 871.

3 “(iii) EXCEPTION.—A term of a mem-  
4 ber of the State and Local Cybersecurity  
5 Resilience Committee shall be three years  
6 if the member is appointed initially to the  
7 Committee upon the establishment of the  
8 Committee.

9 “(iv) TERM REMAINDERS.—Any mem-  
10 ber of the State and Local Cybersecurity  
11 Resilience Committee appointed to fill a  
12 vacancy occurring before the expiration of  
13 the term for which the member’s prede-  
14 cessor was appointed shall be appointed  
15 only for the remainder of such term. A  
16 member may serve after the expiration of  
17 such member’s term until a successor has  
18 taken office.

19 “(v) VACANCIES.—A vacancy in the  
20 State and Local Cybersecurity Resilience  
21 Committee shall be filled in the manner in  
22 which the original appointment was made.

23 “(C) PAY.—Members of the State and  
24 Local Cybersecurity Resilience Committee shall  
25 serve without pay.

1           “(4) CHAIRPERSON; VICE CHAIRPERSON.—The  
2 members of the State and Local Cybersecurity Resilience  
3 Committee shall select a chairperson and vice  
4 chairperson from among members of the committee.

5           “(5) PERMANENT AUTHORITY.—Notwith-  
6 standing section 14 of the Federal Advisory Com-  
7 mittee Act (5 U.S.C. App.), the State and Local Cy-  
8 bersecurity Resilience Committee shall be a perma-  
9 nent authority.

10          “(p) REPORTS.—

11           “(1) ANNUAL REPORTS BY GRANT RECIPI-  
12 ENTS.—

13           “(A) IN GENERAL.—Not later than one  
14 year after an eligible entity or multistate group  
15 receives funds under this section, the eligible  
16 entity or multistate group shall submit to the  
17 Secretary a report on the progress of the eligi-  
18 ble entity or multistate group in implementing  
19 the Cybersecurity Plan of the eligible entity or  
20 Cybersecurity Plans of the eligible entities that  
21 comprise the multistate group, as the case may  
22 be.

23           “(B) ABSENCE OF PLAN.—Not later than  
24 180 days after an eligible entity that does not  
25 have a Cybersecurity Plan receives funds under

1 this section for developing its Cybersecurity  
2 Plan, the eligible entity shall submit to the Sec-  
3 retary a report describing how the eligible enti-  
4 ty obligated and expended grant funds during  
5 the fiscal year to—

6 “(i) so develop such a Cybersecurity  
7 Plan; or

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

10 “(2) ANNUAL REPORTS TO CONGRESS.—Not  
11 less frequently than once per year, the Secretary,  
12 acting through the Director, shall submit to Con-  
13 gress a report on the use of grants awarded under  
14 this section and any progress made toward the fol-  
15 lowing:

16 “(A) Achieving the objectives set forth in  
17 the Homeland Security Strategy to Improve the  
18 Cybersecurity of State, Local, Tribal, and Ter-  
19 ritorial Governments, upon the date on which  
20 the strategy is issued under section 2210.

21 “(B) Developing, implementing, or revising  
22 Cybersecurity Plans.

23 “(C) Reducing cybersecurity risks and cy-  
24 bersecurity threats to information systems, ap-  
25 plications, and user accounts owned or operated



1 by or on behalf of State, local, and Tribal orga-  
2 nizations as a result of the award of such  
3 grants.

4 “(q) AUTHORIZATION OF APPROPRIATIONS.—There  
5 are authorized to be appropriated for grants under this  
6 section—

7 “(1) for each of fiscal years 2022 through  
8 2026, \$500,000,000; and

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

11 **“SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOP-**  
12 **MENT FOR STATE, LOCAL, TRIBAL, AND TER-**  
13 **RITORIAL GOVERNMENT OFFICIALS.**

14 “The Secretary, acting through the Director, shall  
15 develop, regularly update, and maintain a resource guide  
16 for use by State, local, Tribal, and territorial government  
17 officials, including law enforcement officers, to help such  
18 officials identify, prepare for, detect, protect against, re-  
19 spond to, and recover from cybersecurity risks (as such  
20 term is defined in section 2209), cybersecurity threats,  
21 and incidents (as such term is defined in section 2209).”.

22 (b) CLERICAL AMENDMENT.—The table of contents  
23 in section 1(b) of the Homeland Security Act of 2002, as  
24 amended by section 4, is further amended by inserting

1 after the item relating to section 2220 the following new  
2 items:

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

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

3 **SEC. 3. STRATEGY.**

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

9 “(e) HOMELAND SECURITY STRATEGY TO IMPROVE  
10 THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND  
11 TERRITORIAL GOVERNMENTS.—

12 “(1) IN GENERAL.—

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

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

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

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

18           “(2) CONTENTS.—The strategy required under  
19           paragraph (1) shall—

20                   “(A) identify capability gaps in the ability  
21                   of State, local, Tribal, and territorial govern-  
22                   ments to identify, protect against, detect, re-  
23                   spond to, and recover from cybersecurity risks,  
24                   cybersecurity threats, incidents, and  
25                   ransomware incidents;

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

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

16          “(D) identify opportunities to improve the  
17          coordination of the Agency with Federal and  
18          non-Federal entities, such as the Multi-State  
19          Information Sharing and Analysis Center, to  
20          improve—

21                  “(i) incident exercises, information  
22                  sharing and incident notification proce-  
23                  dures;

24                  “(ii) the ability for State, local, Trib-  
25                  al, and territorial governments to volun-

1           tarily adapt and implement guidance in  
2           Federal binding operational directives; and

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

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

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

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

1 risks, cybersecurity threats, incidents, and  
2 ransomware incidents.

3 “(3) CONSIDERATIONS.—In developing the  
4 strategy required under paragraph (1), the Director,  
5 in coordination with the heads of appropriate Fed-  
6 eral agencies, State, local, Tribal, and territorial  
7 governments, the State and Local Cybersecurity Re-  
8 silience Committee established under section 2220A,  
9 and other stakeholders, as appropriate, shall con-  
10 sider—

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 gov-  
17 ernments, including the resulting costs to such  
18 governments;

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 op-  
24 erated by State, local, Tribal, and territorial  
25 governments;

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  
13          CYBERSECURITY AND INFRASTRUCTURE SECURITY AGEN-  
14          CY.—Section 2202 of the Homeland Security Act of 2002  
15          (6 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 fol-  
19               lowing new subsection:

20               “(d) ADDITIONAL RESPONSIBILITIES.—In addition  
21               to 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

1 2220A, for the State and Local Cybersecurity Grant  
2 Program under such section or any other homeland  
3 security assistance administered by the Department  
4 to improve cybersecurity;

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

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

14 “(4) provide education, training, and capacity  
15 development to enhance the security and resilience  
16 of 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  
19 of the Cybersecurity and Infrastructure Security of the  
20 Department of Homeland Security shall conduct a study  
21 to 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.—Sub-  
5 title A of title XXII of the Homeland Security Act  
6 of 2002 (6 U.S.C. 651 et seq.) is amended—

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

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

14 (B) in the second section 2215 (6 U.S.C.  
15 665b; relating to the joint cyber planning of-  
16 fice), by amending the section enumerator and  
17 heading to read as follows:

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

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

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

24 (D) in the fourth section 2215 (6 U.S.C.  
25 665d; relating to Sector Risk Management

1 Agencies), by amending the section enumerator  
2 and heading to read as follows:

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

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

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

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

13 **“SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING**  
14 **PROGRAMS.”.**

15 (2) CONSOLIDATED APPROPRIATIONS ACT,  
16 2021.—Paragraph (1) of section 904(b) of division U  
17 of the Consolidated Appropriations Act, 2021 (Pub-  
18 lic Law 116–260) is amended, in the matter pre-  
19 ceding subparagraph (A), by inserting “of 2002”  
20 after “Homeland Security Act”.

21 (b) CLERICAL AMENDMENT.—The table of contents  
22 in section 1(b) of the Homeland Security Act of 2002 is  
23 amended by striking the items relating to sections 2214  
24 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.

