

116TH CONGRESS  
2D SESSION

# H. R. 5823

---

## AN ACT

To establish a program to make grants to States to address cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or territorial governments, and for other purposes.

1       *Be it enacted by the Senate and House of Representa-*  
2       *tives of the United States of America in Congress assembled,*

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. 2215. STATE AND LOCAL CYBERSECURITY GRANT**  
11 **PROGRAM.**

12       “(a) ESTABLISHMENT.—The Secretary, acting  
13 through the Director, shall establish a program to make  
14 grants to States to address cybersecurity risks and cyber-  
15 security threats to information systems of State, local,  
16 Tribal, or territorial governments (referred to as the  
17 ‘State and Local Cybersecurity Grant Program’ in this  
18 section).

19       “(b) BASELINE REQUIREMENTS.—A grant awarded  
20 under this section shall be used in compliance with the  
21 following:

22               “(1) The Cybersecurity Plan required under  
23 subsection (d) and approved pursuant to subsection  
24 (g).

25               “(2) The Homeland Security Strategy to Im-  
26 prove the Cybersecurity of State, Local, Tribal, and

1 Territorial Governments required in accordance with  
2 section 2210, when issued.

3 “(c) ADMINISTRATION.—The State and Local Cyber-  
4 security Grant Program shall be administered in the same  
5 program office that administers grants made under sec-  
6 tions 2003 and 2004.

7 “(d) ELIGIBILITY.—

8 “(1) IN GENERAL.—A State applying for a  
9 grant under the State and Local Cybersecurity  
10 Grant Program shall submit to the Secretary a Cy-  
11 bersecurity Plan for approval. Such plan shall—

12 “(A) incorporate, to the extent practicable,  
13 any existing plans of such State to protect  
14 against cybersecurity risks and cybersecurity  
15 threats to information systems of State, local,  
16 Tribal, or territorial governments;

17 “(B) describe, to the extent practicable,  
18 how such State shall—

19 “(i) enhance the preparation, re-  
20 sponse, and resiliency of information sys-  
21 tems owned or operated by such State or,  
22 if appropriate, by local, Tribal, or terri-  
23 torial governments, against cybersecurity  
24 risks and cybersecurity threats;

1           “(ii) 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           in information systems of such State, local,  
7           Tribal, or territorial governments;

8           “(iii) ensure that State, local, Tribal,  
9           and territorial governments that own or  
10          operate information systems within the  
11          State adopt best practices and methodolo-  
12          gies to enhance cybersecurity, such as the  
13          practices set forth in the cybersecurity  
14          framework developed by the National Insti-  
15          tute of Standards and Technology;

16          “(iv) promote the delivery of safe, rec-  
17          ognizable, and trustworthy online services  
18          by State, local, Tribal, and territorial gov-  
19          ernments, including through the use of the  
20          .gov internet domain;

21          “(v) mitigate any identified gaps in  
22          the State, local, Tribal, or territorial gov-  
23          ernment cybersecurity workforces, enhance  
24          recruitment and retention efforts for such  
25          workforces, and bolster the knowledge,

1 skills, and abilities of State, local, Tribal,  
2 and territorial government personnel to ad-  
3 dress cybersecurity risks and cybersecurity  
4 threats;

5 “(vi) ensure continuity of communica-  
6 tions and data networks within such State  
7 between such State and local, Tribal, and  
8 territorial governments that own or operate  
9 information systems within such State in  
10 the event of an incident involving such  
11 communications or data networks within  
12 such State;

13 “(vii) assess and mitigate, to the  
14 greatest degree possible, cybersecurity  
15 risks and cybersecurity threats related to  
16 critical infrastructure and key resources,  
17 the degradation of which may impact the  
18 performance of information systems within  
19 such State;

20 “(viii) enhance capability to share  
21 cyber threat indicators and related infor-  
22 mation between such State and local, Trib-  
23 al, and territorial governments that own or  
24 operate information systems within such  
25 State; and

1 “(ix) develop and coordinate strategies  
2 to address cybersecurity risks and cyberse-  
3 curity threats in consultation with—

4 “(I) local, Tribal, and territorial  
5 governments within the State; and

6 “(II) as applicable—

7 “(aa) neighboring States or,  
8 as appropriate, members of an  
9 information sharing and analysis  
10 organization; and

11 “(bb) neighboring countries;  
12 and

13 “(C) include, to the extent practicable, an  
14 inventory of the information technology de-  
15 ployed on the information systems owned or op-  
16 erated by such State or by local, Tribal, or ter-  
17 ritorial governments within such State, includ-  
18 ing legacy information technology that is no  
19 longer supported by the manufacturer.

20 “(e) PLANNING COMMITTEES.—

21 “(1) IN GENERAL.—A State applying for a  
22 grant under this section shall establish a cybersecu-  
23 rity planning committee to assist in the following:

1           “(A) The development, implementation,  
2           and revision of such State’s Cybersecurity Plan  
3           required under subsection (d).

4           “(B) The determination of effective fund-  
5           ing priorities for such grant in accordance with  
6           subsection (f).

7           “(2) COMPOSITION.—Cybersecurity planning  
8           committees described in paragraph (1) shall be com-  
9           prised of representatives from counties, cities, towns,  
10          and Tribes within the State receiving a grant under  
11          this section, including, as appropriate, representa-  
12          tives of rural, suburban, and high-population juris-  
13          dictions.

14          “(3) RULE OF CONSTRUCTION REGARDING EX-  
15          ISTING PLANNING COMMITTEES.—Nothing in this  
16          subsection may be construed to require that any  
17          State establish a cybersecurity planning committee if  
18          such State has established and uses a multijuris-  
19          dictional planning committee or commission that  
20          meets the requirements of this paragraph.

21          “(f) USE OF FUNDS.—A State that receives a grant  
22          under this section shall use the grant to implement such  
23          State’s Cybersecurity Plan, or to assist with activities de-  
24          termined by the Secretary, in consultation with the Direc-  
25          tor, to be integral to address cybersecurity risks and cy-

1 bersecurity threats to information systems of State, local,  
2 Tribal, or territorial governments, as the case may be.

3 “(g) APPROVAL OF PLANS.—

4 “(1) APPROVAL AS CONDITION OF GRANT.—Be-  
5 fore a State may receive a grant under this section,  
6 the Secretary, acting through the Director, shall re-  
7 view and approve such State’s Cybersecurity Plan  
8 required under subsection (d).

9 “(2) PLAN REQUIREMENTS.—In approving a  
10 Cybersecurity Plan under this subsection, the Direc-  
11 tor shall ensure such Plan—

12 “(A) meets the requirements specified in  
13 subsection (d); and

14 “(B) upon issuance of the Homeland Secu-  
15 rity Strategy to Improve the Cybersecurity of  
16 State, Local, Tribal, and Territorial Govern-  
17 ments authorized pursuant to section 2210,  
18 complies, as appropriate, with the goals and ob-  
19 jectives of such Strategy.

20 “(3) APPROVAL OF REVISIONS.—The Secretary,  
21 acting through the Director, may approve revisions  
22 to a Cybersecurity Plan as the Director determines  
23 appropriate.

24 “(4) EXCEPTION.—Notwithstanding the re-  
25 quirement under subsection (d) to submit a Cyberse-



1       curity Plan as a condition of apply for a grant under  
2       this section, such a grant may be awarded to a State  
3       that has not so submitted a Cybersecurity Plan to  
4       the Secretary if—

5               “(A) such State certifies to the Secretary  
6               that it will submit to the Secretary a Cyberse-  
7               curity Plan for approval by September 30,  
8               2022;

9               “(B) such State certifies to the Secretary  
10              that the activities that will be supported by  
11              such grant are integral to the development of  
12              such Cybersecurity Plan; or

13              “(C) such State certifies to the Secretary,  
14              and the Director confirms, that the activities  
15              that will be supported by the grant will address  
16              imminent cybersecurity risks or cybersecurity  
17              threats to the information systems of such  
18              State or of a local, Tribal, or territorial govern-  
19              ment in such State.

20       “(h) LIMITATIONS ON USES OF FUNDS.—

21               “(1) IN GENERAL.—A State that receives a  
22       grant under this section may not use such grant—

23               “(A) to supplant State, local, Tribal, or  
24       territorial funds;

1           “(B) for any recipient cost-sharing con-  
2           tribution;

3           “(C) to pay a demand for ransom in an at-  
4           tempt to regain access to information or an in-  
5           formation system of such State or of a local,  
6           Tribal, or territorial government in such State;

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

8           “(E) for any purpose that does not directly  
9           address cybersecurity risks or cybersecurity  
10          threats on an information systems of such State  
11          or of a local, Tribal, or territorial government  
12          in such State.

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

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

23          “(j) APPORTIONMENT.—For fiscal year 2020 and  
24          each fiscal year thereafter, the Secretary shall apportion

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

3 “(1) BASELINE AMOUNT.—The Secretary shall  
4 first apportion 0.25 percent of such amounts to each  
5 of American Samoa, the Commonwealth of the  
6 Northern Mariana Islands, Guam, and the Virgin Is-  
7 lands, and 0.75 percent of such amounts to each of  
8 the remaining States.

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

12 “(A) the population of each State; bears to

13 “(B) the population of all States.

14 “(k) FEDERAL SHARE.—The Federal share of the  
15 cost of an activity carried out using funds made available  
16 under the program may not exceed the following percent-  
17 ages:

18 “(1) For fiscal year 2021, 90 percent.

19 “(2) For fiscal year 2022, 80 percent.

20 “(3) For fiscal year 2023, 70 percent.

21 “(4) For fiscal year 2024, 60 percent.

22 “(5) For fiscal year 2025 and each subsequent  
23 fiscal year, 50 percent.

24 “(l) STATE RESPONSIBILITIES.—

1           “(1) CERTIFICATION.—Each State that receives  
2           a grant under this section shall certify to the Sec-  
3           retary that the grant will be used for the purpose for  
4           which the grant is awarded and in compliance with  
5           the Cybersecurity Plan or other purpose approved by  
6           the Secretary under subsection (g).

7           “(2) AVAILABILITY OF FUNDS TO LOCAL, TRIB-  
8           AL, AND TERRITORIAL GOVERNMENTS.—Not later  
9           than 45 days after a State receives a grant under  
10          this section, such State shall, without imposing un-  
11          reasonable or unduly burdensome requirements as a  
12          condition of receipt, obligate or otherwise make  
13          available to local, Tribal, and territorial governments  
14          in such State, consistent with the applicable Cyber-  
15          security Plan—

16               “(A) not less than 80 percent of funds  
17               available under such grant;

18               “(B) with the consent of such local, Tribal,  
19               and territorial governments, items, services, ca-  
20               pabilities, or activities having a value of not less  
21               than 80 percent of the amount of the grant; or

22               “(C) with the consent of the local, Tribal,  
23               and territorial governments, grant funds com-  
24               bined with other items, services, capabilities, or

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

3 “(3) CERTIFICATIONS REGARDING DISTRIBUTION OF GRANT FUNDS TO LOCAL, TRIBAL, TERRITORIAL GOVERNMENTS.—A State shall certify to the  
4 Secretary that the State has made the distribution  
5 to local, Tribal, and territorial governments required  
6 under paragraph (2).  
7

8 “(4) EXTENSION OF PERIOD.—A State may request in writing that the Secretary extend the period  
9 of time specified in paragraph (2) for an additional  
10 period of time. The Secretary may approve such a  
11 request if the Secretary determines such extension is  
12 necessary to ensure the obligation and expenditure  
13 of grant funds align with the purpose of the grant  
14 program.  
15

16 “(5) EXCEPTION.—Paragraph (2) shall not  
17 apply to the District of Columbia, the Commonwealth of Puerto Rico, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam,  
18 or the Virgin Islands.  
19

20 “(6) DIRECT FUNDING.—If a State does not  
21 make the distribution to local, Tribal, or territorial  
22 governments in such State required under paragraph  
23  
24

1       (2), such a local, Tribal, or territorial government  
2       may petition the Secretary.

3           “(7) PENALTIES.—In addition to other remedies available to the Secretary, the Secretary may  
4       terminate or reduce the amount of a grant awarded  
5       under this section to a State or transfer grant funds  
6       previously awarded to such State directly to the appropriate local, Tribal, or territorial government if  
7       such State violates a requirement of this subsection.

8       “(m) ADVISORY COMMITTEE.—

9           “(1) ESTABLISHMENT.—The Director shall establish a State and Local Cybersecurity Resiliency  
10       Committee to provide State, local, Tribal, and territorial stakeholder expertise, situational awareness,  
11       and recommendations to the Director, as appropriate, regarding how to—

12           “(A) address cybersecurity risks and cybersecurity threats to information systems of  
13       State, local, Tribal, or territorial governments;  
14       and

15           “(B) improve the ability of such governments to prevent, protect against, respond,  
16       mitigate, and recover from cybersecurity risks  
17       and cybersecurity threats.

1           “(2) DUTIES.—The State and Local Cybersecu-  
2       rity Resiliency Committee shall—

3           “(A) submit to the Director recommenda-  
4       tions that may inform guidance for applicants  
5       for grants under this section;

6           “(B) upon the request of the Director, pro-  
7       vide to the Director technical assistance to in-  
8       form the review of Cybersecurity Plans sub-  
9       mitted by applicants for grants under this sec-  
10      tion, and, as appropriate, submit to the Direc-  
11      tor recommendations to improve such Plans  
12      prior to the Director’s determination regarding  
13      whether to approve such Plans;

14          “(C) advise and provide to the Director  
15      input regarding the Homeland Security Strat-  
16      egy to Improve Cybersecurity for State, Local,  
17      Tribal, and Territorial Governments required  
18      under section 2210; and

19          “(D) upon the request of the Director, pro-  
20      vide to the Director recommendations, as ap-  
21      propriate, regarding how to—

22              “(i) address cybersecurity risks and  
23              cybersecurity threats on information sys-  
24              tems of State, local, Tribal, or territorial  
25              governments;

1 “(ii) and improve the cybersecurity re-  
2 silience of such governments.

3 “(3) MEMBERSHIP.—

4 “(A) NUMBER AND APPOINTMENT.—The  
5 State and Local Cybersecurity Resiliency Com-  
6 mittee shall be composed of 15 members ap-  
7 pointed by the Director, as follows:

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

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

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

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

20 “(v) Two individuals recommended to  
21 the Director by the National League of  
22 Cities.

23 “(vi) One individual recommended to  
24 the Director by the United States Con-  
25 ference of Mayors.



1           “(vii) One individual recommended to  
2           the Director by the Multi-State Informa-  
3           tion Sharing and Analysis Center.

4           “(viii) Four individuals who have edu-  
5           cational and professional experience related  
6           to cybersecurity analysis or policy.

7           “(B) TERMS.—Each member of the State  
8           and Local Cybersecurity Resiliency Committee  
9           shall be appointed for a term of two years, ex-  
10          cept that such term shall be three years only in  
11          the case of members who are appointed initially  
12          to the Committee upon the establishment of the  
13          Committee. Any member appointed to fill a va-  
14          cancy occurring before the expiration of the  
15          term for which the member’s predecessor was  
16          appointed shall be appointed only for the re-  
17          mainder of such term. A member may serve  
18          after the expiration of such member’s term  
19          until a successor has taken office. A vacancy in  
20          the Commission shall be filled in the manner in  
21          which the original appointment was made.

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

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

5           “(5) FEDERAL ADVISORY COMMITTEE ACT.—  
6       The Federal Advisory Committee Act (5 U.S.C.  
7       App.) shall not apply to the State and Local Cyber-  
8       security Resilience Committee.

9           “(n) REPORTS.—

10          “(1) ANNUAL REPORTS BY STATE GRANT RE-  
11       CIPIENTS.—A State that receives a grant under this  
12       section shall annually submit to the Secretary a re-  
13       port on the progress of the State in implementing  
14       the Cybersecurity Plan approved pursuant to sub-  
15       section (g). If the State does not have a Cybersecu-  
16       rity Plan approved pursuant to subsection (g), the  
17       State shall submit to the Secretary a report describ-  
18       ing how grant funds were obligated and expended to  
19       develop a Cybersecurity Plan or improve the cyberse-  
20       curity of information systems owned or operated by  
21       State, local, Tribal, or territorial governments in  
22       such State. The Secretary, acting through the Direc-  
23       tor, shall make each such report publicly available,  
24       including by making each such report available on  
25       the internet website of the Agency, subject to any

1 redactions the Director determines necessary to pro-  
2 tect classified or other sensitive information.

3 “(2) ANNUAL REPORTS TO CONGRESS.—At  
4 least once each year, the Secretary, acting through  
5 the Director, shall submit to Congress a report on  
6 the use of grants awarded under this section and  
7 any progress made toward the following:

8 “(A) Achieving the objectives set forth in  
9 the Homeland Security Strategy to Improve the  
10 Cybersecurity of State, Local, Tribal, and Ter-  
11 ritorial Governments, upon the strategy’s  
12 issuance under section 2210.

13 “(B) Developing, implementing, or revising  
14 Cybersecurity Plans.

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

20 “(o) AUTHORIZATION OF APPROPRIATIONS.—There  
21 are authorized to be appropriated for grants under this  
22 section—

23 “(1) for each of fiscal years 2021 through  
24 2025, \$400,000,000; and

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

3           “(p) DEFINITIONS.—In this section:

4           “(1) CRITICAL INFRASTRUCTURE.—The term  
5 ‘critical infrastructure’ has the meaning given that  
6 term in section 2.

7           “(2) CYBER THREAT INDICATOR.—The term  
8 ‘cyber threat indicator’ has the meaning given such  
9 term in section 102 of the Cybersecurity Act of  
10 2015.

11           “(3) DIRECTOR.—The term ‘Director’ means  
12 the Director of the Cybersecurity and Infrastructure  
13 Security Agency.

14           “(4) INCIDENT.—The term ‘incident’ has the  
15 meaning given such term in section 2209.

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

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

1           “(7) KEY RESOURCES.—The term ‘key re-  
2       sources’ has the meaning given that term in section  
3       2.

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

8           “(9) STATE.—The term ‘State’—

9               “(A) means each of the several States, the  
10           District of Colombia, and the territories and  
11           possessions of the United States; and

12               “(B) includes any federally recognized In-  
13           dian tribe that notifies the Secretary, not later  
14           than 120 days after the date of the enactment  
15           of this section or not later than 120 days before  
16           the start of any fiscal year in which a grant  
17           under this section is awarded, that the tribe in-  
18           tends to develop a Cybersecurity Plan and  
19           agrees to forfeit any distribution under sub-  
20           section (l)(2).

21   **“SEC. 2216. CYBERSECURITY RESOURCE GUIDE DEVELOP-**  
22               **MENT FOR STATE, LOCAL, TRIBAL, AND TER-**  
23               **RITORIAL GOVERNMENT OFFICIALS.**

24           “The Secretary, acting through the Director, shall  
25   develop a resource guide for use by State, local, Tribal,

1 and territorial government officials, including law enforce-  
 2 ment officers, to help such officials identify, prepare for,  
 3 detect, protect against, respond to, and recover from cy-  
 4 bersecurity risks, cybersecurity threats, and incidents (as  
 5 such term is defined in section 2209).”.

6 (b) CLERICAL AMENDMENT.—The table of contents  
 7 in section 1(b) of the Homeland Security Act of 2002 is  
 8 amended by inserting after the item relating to section  
 9 2214 the following new items:

“Sec. 2215. State and Local Cybersecurity Grant Program.

“Sec. 2216. Cybersecurity resource guide development for State, local, Tribal,  
 and territorial government officials.”.

### 10 **SEC. 3. STRATEGY.**

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

16 “(e) HOMELAND SECURITY STRATEGY TO IMPROVE  
 17 THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND  
 18 TERRITORIAL GOVERNMENTS.—

19 “(1) IN GENERAL.—Not later than 270 days  
 20 after the date of the enactment of this subsection,  
 21 the Secretary, acting through the Director, shall, in  
 22 coordination with appropriate Federal departments  
 23 and agencies, State, local, Tribal, and territorial  
 24 governments, the State and Local Cybersecurity Re-

1       silience Committee (established under section 2215),  
2       and other stakeholders, as appropriate, develop and  
3       make publicly available a Homeland Security Strat-  
4       egy to Improve the Cybersecurity of State, Local,  
5       Tribal, and Territorial Governments that provides  
6       recommendations regarding how the Federal Gov-  
7       ernment should support and promote the ability  
8       State, local, Tribal, and territorial governments to  
9       identify, protect against, detect respond to, and re-  
10      cover from cybersecurity risks, cybersecurity threats,  
11      and incidents (as such term is defined in section  
12      2209) and establishes baseline requirements and  
13      principles to which Cybersecurity Plans under such  
14      section shall be aligned.

15           “(2) CONTENTS.—The Homeland Security  
16      Strategy to Improve the Cybersecurity of State,  
17      Local, Tribal, and Territorial Governments required  
18      under paragraph (1) shall—

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

24           “(B) identify Federal resources and capa-  
25      bilities that are available or could be made

1 available to State, local, Tribal, and territorial  
2 governments to help such governments identify,  
3 protect against, detect, respond to, and recover  
4 from cybersecurity risks, cybersecurity threats,  
5 and incidents;

6 “(C) identify and assess the limitations of  
7 Federal resources and capabilities available to  
8 State, local, Tribal, and territorial governments  
9 to help such governments identify, protect  
10 against, detect, respond to, and recover from  
11 cybersecurity risks, cybersecurity threats, and  
12 incidents, and make recommendations to ad-  
13 dress such limitations;

14 “(D) identify opportunities to improve the  
15 Agency’s coordination with Federal and non-  
16 Federal entities, such as the Multi-State Infor-  
17 mation Sharing and Analysis Center, to im-  
18 prove incident exercises, information sharing  
19 and incident notification procedures, the ability  
20 for State, local, Tribal, and territorial govern-  
21 ments to voluntarily adapt and implement guid-  
22 ance in Federal binding operational directives,  
23 and opportunities to leverage Federal schedules  
24 for cybersecurity investments under section 502  
25 of title 40, United States Code;



1           “(E) recommend new initiatives the Fed-  
2           eral Government should undertake to improve  
3           the ability of State, local, Tribal, and territorial  
4           governments to help such governments identify,  
5           protect against, detect, respond to, and recover  
6           from cybersecurity risks, cybersecurity threats,  
7           and incidents;

8           “(F) set short-term and long-term goals  
9           that will improve the ability of State, local,  
10          Tribal, and territorial governments to help such  
11          governments identify, protect against, detect,  
12          respond to, and recover from cybersecurity  
13          risks, cybersecurity threats, and incidents; and

14          “(G) set dates, including interim bench-  
15          marks, as appropriate for State, local, Tribal,  
16          territorial governments to establish baseline ca-  
17          pabilities to identify, protect against, detect, re-  
18          spond to, and recover from cybersecurity risks,  
19          cybersecurity threats, and incidents.

20          “(3) CONSIDERATIONS.—In developing the  
21          Homeland Security Strategy to Improve the Cyber-  
22          security of State, Local, Tribal, and Territorial Gov-  
23          ernments required under paragraph (1), the Direc-  
24          tor, in coordination with appropriate Federal depart-  
25          ments and agencies, State, local, Tribal, and terri-

1       torial governments, the State and Local Cybersecu-  
2       rity Resilience Committee, and other stakeholders,  
3       as appropriate, shall consider—

4               “(A) lessons learned from incidents that  
5       have affected State, local, Tribal, and territorial  
6       governments, and exercises with Federal and  
7       non-Federal entities;

8               “(B) the impact of incidents that have af-  
9       fected State, local, Tribal, and territorial gov-  
10      ernments, including the resulting costs to such  
11      governments;

12              “(C) the information related to the interest  
13      and ability of state and non-state threat actors  
14      to compromise information systems owned or  
15      operated by State, local, Tribal, and territorial  
16      governments;

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

21              “(E) recommendations made by the State  
22      and Local Cybersecurity Resilience Com-  
23      mittee.”.

24       (b) RESPONSIBILITIES OF THE DIRECTOR OF THE  
25      CYBERSECURITY AND INFRASTRUCTURE SECURITY AGEN-

1 CY.—Subsection (c) of section 2202 of the Homeland Se-  
2 curity Act of 2002 (6 U.S.C. 652) is amended—

3 (1) by redesignating paragraphs (6) through  
4 (11) as paragraphs (11) through (16), respectively;  
5 and

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

8 “(6) develop program guidance, in consultation  
9 with the State and Local Government Cybersecurity  
10 Resiliency Committee established under section  
11 2215, for the State and Local Cybersecurity Grant  
12 Program under such section or any other homeland  
13 security assistance administered by the Department  
14 to improve cybersecurity;

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

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

1           “(9) provide education, training, and capacity  
2           development to enhance the security and resilience  
3           of cybersecurity and infrastructure security;

4           “(10) provide information to State, local, Trib-  
5           al, and territorial governments on the security bene-  
6           fits of .gov domain name registration services;”.

7           (c) FEASIBILITY STUDY.—Not later than 180 days  
8           after the date of the enactment of this Act, the Director  
9           of the Cybersecurity and Infrastructure Security Agency  
10          of the Department of Homeland Security shall conduct a  
11          study to assess the feasibility of implementing a short-  
12          term rotational program for the detail of approved State,  
13          local, Tribal, and territorial government employees in  
14          cyber workforce positions to the Agency.

          Passed the House of Representatives September 30,  
2020.

Attest:

*Clerk.*



116TH CONGRESS  
2D SESSION

# H. R. 5823

---

## AN ACT

To establish a program to make grants to States to address cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or territorial governments, and for other purposes.