

116TH CONGRESS  
2D SESSION

# H. R. 5823

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.

---

## IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 10, 2020

Mr. RICHMOND (for himself, Mr. KATKO, Mr. KILMER, Mr. McCAUL, Mr. RUPPERSBERGER, Mr. THOMPSON of Mississippi, Mr. ROGERS of Alabama, Ms. SLOTKIN, Mr. ROSE of New York, Mr. PAYNE, Mrs. WATSON COLEMAN, Mr. LANGEVIN, Mr. CLEAVER, Ms. UNDERWOOD, and Ms. TITUS) introduced the following bill; which was referred to the Committee on Homeland Security

---

## A BILL

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,*

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 section:

6 **“SEC. 2215. STATE AND LOCAL CYBERSECURITY GRANT**  
7 **PROGRAM.**

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

15 “(b) BASELINE REQUIREMENTS.—A grant awarded  
16 under this section shall be used in compliance with the  
17 following:

18 “(1) The Cybersecurity Plan required under  
19 subsection (d) and approved pursuant to subsection  
20 (g).

21 “(2) The Homeland Security Strategy to Im-  
22 prove the Cybersecurity of State, Local, Tribal, and  
23 Territorial Governments required in accordance with  
24 section 2210, when issued.

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

1 program office that administers grants made under sec-  
2 tions 2003 and 2004.

3 “(d) ELIGIBILITY.—

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

8 “(A) incorporate, to the extent practicable,  
9 any existing plans of such State to protect  
10 against cybersecurity risks and cybersecurity  
11 threats to information systems of State, local,  
12 Tribal, or territorial governments;

13 “(B) describe, to the extent practicable,  
14 how such State shall—

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

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

1 in information systems of such State, local,  
2 Tribal, or territorial governments;

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

11 “(iv) mitigate any identified gaps in  
12 the State, local, Tribal, or territorial gov-  
13 ernment cybersecurity workforces, enhance  
14 recruitment and retention efforts for such  
15 workforces, and bolster the knowledge,  
16 skills, and abilities of State, local, Tribal,  
17 and territorial government personnel to ad-  
18 dress cybersecurity risks and cybersecurity  
19 threats;

20 “(v) ensure continuity of communica-  
21 tions and data networks within such State  
22 between such State and local, Tribal, and  
23 territorial governments that own or operate  
24 information systems within such State in  
25 the event of an incident involving such

1           communications or data networks within  
2           such State;

3           “(vi) assess and mitigate, to the  
4           greatest degree possible, cybersecurity  
5           risks and cybersecurity threats related to  
6           critical infrastructure and key resources,  
7           the degradation of which may impact the  
8           performance of information systems within  
9           such State;

10          “(vii) enhance capability to share  
11          cyber threat indicators and related infor-  
12          mation between such State and local, Trib-  
13          al, and territorial governments that own or  
14          operate information systems within such  
15          State; and

16          “(viii) develop and coordinate strate-  
17          gies to address cybersecurity risks in con-  
18          sultation with—

19                 “(I) local, Tribal, and territorial  
20                 governments within the State; and

21                 “(II) as applicable—

22                         “(aa) neighboring States or,  
23                         as appropriate, members of an  
24                         information sharing and analysis  
25                         organization; and

1                                   “(bb) neighboring countries;  
2                                   and

3                                   “(C) include, to the extent practicable, an  
4                                   inventory of the information technology de-  
5                                   ployed on the information systems owned or op-  
6                                   erated by such State or by local, Tribal, or ter-  
7                                   ritorial governments within such State, includ-  
8                                   ing legacy information technology that is no  
9                                   longer supported by the manufacturer.

10                                  “(e) PLANNING COMMITTEES.—

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

14   “(A) The development, implementation,  
15   and revision of such State’s Cybersecurity Plan  
16   required under subsection (d).

17   “(B) The determination of effective fund-  
18   ing priorities for such grant in accordance with  
19   subsection (f).

20                                  “(2) COMPOSITION.—Cybersecurity planning  
21                                  committees described in paragraph (1) shall be com-  
22                                  prised of representatives from counties, cities, towns,  
23                                  and Tribes within the State receiving a grant under  
24                                  this section, including, as appropriate, representa-

1 tives of rural, suburban, and high-population juris-  
2 dictions.

3 “(3) RULE OF CONSTRUCTION REGARDING EX-  
4 ISTING PLANNING COMMITTEES.—Nothing in this  
5 subsection may be construed to require that any  
6 State establish a cybersecurity planning committee if  
7 such State has established and uses a multijuris-  
8 dictional planning committee or commission that  
9 meets the requirements of this paragraph.

10 “(f) USE OF FUNDS.—A State that receives a grant  
11 under this section shall use the grant to implement such  
12 State’s Cybersecurity Plan, or to assist with activities de-  
13 termined by the Secretary, in consultation with the Direc-  
14 tor, to be integral to address cybersecurity risks and cy-  
15 bersecurity threats to information systems of State, local,  
16 Tribal, or territorial governments, as the case may be.

17 “(g) APPROVAL OF PLANS.—

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

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

1           “(A) meets the requirements specified in  
2 subsection (d); and

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

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

13           “(4) EXCEPTION.—Notwithstanding the re-  
14 quirement under subsection (d) to submit a Cyberse-  
15 curity Plan as a condition of apply for a grant under  
16 this section, such a grant may be awarded to a State  
17 that has not so submitted a Cybersecurity Plan to  
18 the Secretary if—

19           “(A) such State certifies to the Secretary  
20 that it will submit to the Secretary a Cyberse-  
21 curity Plan for approval by September 30,  
22 2022;

23           “(B) such State certifies to the Secretary  
24 that the activities that will be supported by



1 such grant are integral to the development of  
2 such Cybersecurity Plan; or

3 “(C) such State certifies to the Secretary,  
4 and the Director confirms, that the activities  
5 that will be supported by the grant will address  
6 imminent cybersecurity risks or cybersecurity  
7 threats to the information systems of such  
8 State or of a local, Tribal, or territorial govern-  
9 ment in such State.

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

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

13 “(A) to supplant State, local, Tribal, or  
14 territorial funds;

15 “(B) for any recipient cost-sharing con-  
16 tribution;

17 “(C) to pay a demand for ransom in an at-  
18 tempt to regain access to information or an in-  
19 formation system of such State or of a local,  
20 Tribal, or territorial government in such State;

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

22 “(E) for any purpose that does not directly  
23 address cybersecurity risks or cybersecurity  
24 threats on an information systems of such State

1           or of a local, Tribal, or territorial government  
2           in such State.

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

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

13          “(j) APPORTIONMENT.—For fiscal year 2020 and  
14          each fiscal year thereafter, the Secretary shall apportion  
15          amounts appropriated to carry out this section among  
16          States as follows:

17                 “(1) BASELINE AMOUNT.—The Secretary shall  
18                 first apportion 0.25 percent of such amounts to each  
19                 of American Samoa, the Commonwealth of the  
20                 Northern Mariana Islands, Guam, and the Virgin Is-  
21                 lands, and 0.75 percent of such amounts to each of  
22                 the remaining States.

23                 “(2) REMAINDER.—The Secretary shall appor-  
24                 tion the remainder of such amounts in the ratio  
25                 that—

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

2           “(B) the population of all States.

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

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

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

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

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

11          “(5) For fiscal year 2025 and each subsequent  
12 fiscal year, 50 percent.

13          “(l) STATE RESPONSIBILITIES.—

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

20           “(2) AVAILABILITY OF FUNDS TO LOCAL, TRIB-  
21 AL, AND TERRITORIAL GOVERNMENTS.—Not later  
22 than 45 days after a State receives a grant under  
23 this section, such State shall, without imposing un-  
24 reasonable or unduly burdensome requirements as a  
25 condition of receipt, obligate or otherwise make

1 available to local, Tribal, and territorial governments  
2 in such State, consistent with the applicable Cyber-  
3 security Plan—

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

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

10 “(C) with the consent of the local, Tribal,  
11 and territorial governments, grant funds com-  
12 bined with other items, services, capabilities, or  
13 activities having the total value of not less than  
14 80 percent of the amount of the grant.

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

19 “(4) EXTENSION OF PERIOD.—A State may re-  
20 quest in writing that the Secretary extend the period  
21 of time specified in paragraph (2) for an additional  
22 period of time. The Secretary may approve such a  
23 request if the Secretary determines such extension is  
24  
25

1 necessary to ensure the obligation and expenditure  
2 of grant funds align with the purpose of the grant  
3 program.

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

9 “(6) DIRECT FUNDING.—If a State does not  
10 make the distribution to local, Tribal, or territorial  
11 governments in such State required under paragraph  
12 (2), such a local, Tribal, or territorial government  
13 may petition the Secretary.

14 “(7) PENALTIES.—In addition to other rem-  
15 edies available to the Secretary, the Secretary may  
16 terminate or reduce the amount of a grant awarded  
17 under this section to a State or transfer grant funds  
18 previously awarded to such State directly to the ap-  
19 propriate local, Tribal, or territorial government if  
20 such State violates a requirement of this subsection.

21 “(m) ADVISORY COMMITTEE.—

22 “(1) ESTABLISHMENT.—The Director shall es-  
23 tablish a State and Local Cybersecurity Resiliency  
24 Committee to provide State, local, Tribal, and terri-  
25 torial stakeholder expertise, situational awareness,

1 and recommendations to the Director, as appro-  
2 priate, regarding how to—

3 “(A) address cybersecurity risks and cyber-  
4 security threats to information systems of  
5 State, local, Tribal, or territorial governments;  
6 and

7 “(B) improve the ability of such govern-  
8 ments to prevent, protect against, respond,  
9 mitigate, and recover from cybersecurity risks  
10 and cybersecurity threats.

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

13 “(A) submit to the Director recommenda-  
14 tions that may inform guidance for applicants  
15 for grants under this section;

16 “(B) upon the request of the Director, pro-  
17 vide to the Director technical assistance to in-  
18 form the review of Cybersecurity Plans sub-  
19 mitted by applicants for grants under this sec-  
20 tion, and, as appropriate, submit to the Direc-  
21 tor recommendations to improve such Plans  
22 prior to the Director’s determination regarding  
23 whether to approve such Plans;

24 “(C) advise and provide to the Director  
25 input regarding the Homeland Security Strat-

1           egy to Improve Cybersecurity for State, Local,  
2           Tribal, and Territorial Governments required  
3           under section 2210; and

4           “(D) upon the request of the Director, pro-  
5           vide to the Director recommendations, as ap-  
6           propriate, regarding how to—

7           “(i) address cybersecurity risks and  
8           cybersecurity threats on information sys-  
9           tems of State, local, Tribal, or territorial  
10          governments;

11          “(ii) and improve the cybersecurity re-  
12          silience of such governments.

13          “(3) MEMBERSHIP.—

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

18          “(i) Two individuals recommended to  
19          the Director by the National Governors As-  
20          sociation.

21          “(ii) Two individuals recommended to  
22          the Director by the National Association of  
23          State Chief Information Officers.

1           “(iii) One individual recommended to  
2           the Director by the National Guard Bu-  
3           reau.

4           “(iv) Two individuals recommended to  
5           the Director by the National Association of  
6           Counties.

7           “(v) Two individuals recommended to  
8           the Director by the National League of  
9           Cities.

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

13          “(vii) One individual recommended to  
14          the Director by the Multi-State Informa-  
15          tion Sharing and Analysis Center.

16          “(viii) Four individuals who have edu-  
17          cational and professional experience related  
18          to cybersecurity analysis or policy.

19          “(B) TERMS.—Each member of the State  
20          and Local Cybersecurity Resiliency Committee  
21          shall be appointed for a term of two years, ex-  
22          cept that such term shall be three years only in  
23          the case of members who are appointed initially  
24          to the Committee upon the establishment of the  
25          Committee. Any member appointed to fill a va-



1           cancy occurring before the expiration of the  
2           term for which the member's predecessor was  
3           appointed shall be appointed only for the re-  
4           mainder of such term. A member may serve  
5           after the expiration of such member's term  
6           until a successor has taken office. A vacancy in  
7           the Commission shall be filled in the manner in  
8           which the original appointment was made.

9           “(C) PAY.—Members of the State and  
10          Local Cybersecurity Resiliency Committee shall  
11          serve without pay.

12          “(4) CHAIRPERSON; VICE CHAIRPERSON.—The  
13          members of the State and Local Cybersecurity Resili-  
14          ency Committee shall select a chairperson and vice  
15          chairperson from among Committee members.

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

20          “(n) REPORTS.—

21          “(1) ANNUAL REPORTS BY STATE GRANT RE-  
22          CIPIENTS.—A State that receives a grant under this  
23          section shall annually submit to the Secretary a re-  
24          port on the progress of the State in implementing  
25          the Cybersecurity Plan approved pursuant to sub-

1 section (g). If the State does not have a Cybersecu-  
2 rity Plan approved pursuant to subsection (g), the  
3 State shall submit to the Secretary a report describ-  
4 ing how grant funds were obligated and expended to  
5 develop a Cybersecurity Plan or improve the cyberse-  
6 curity of information systems owned or operated by  
7 State, local, Tribal, or territorial governments in  
8 such State. The Secretary, acting through the Direc-  
9 tor, shall make each such report publicly available,  
10 including by making each such report available on  
11 the internet website of the Agency, subject to any  
12 redactions the Director determines necessary to pro-  
13 tect classified or other sensitive information.

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

19 “(A) Achieving the objectives set forth in  
20 the Homeland Security Strategy to Improve the  
21 Cybersecurity of State, Local, Tribal, and Ter-  
22 ritorial Governments, upon the strategy’s  
23 issuance under section 2210.

24 “(B) Developing, implementing, or revising  
25 Cybersecurity Plans.

1           “(C) Reducing cybersecurity risks and cy-  
2           bersecurity threats to information systems  
3           owned or operated by State, local, Tribal, and  
4           territorial governments as a result of the award  
5           of such grants.

6           “(o) AUTHORIZATION OF APPROPRIATIONS.—There  
7           are authorized to be appropriated for grants under this  
8           section—

9           “(1) for each of fiscal years 2021 through  
10          2025, \$400,000,000; and

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

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

14          “(1) CRITICAL INFRASTRUCTURE.—The term  
15          ‘critical infrastructure’ has the meaning given that  
16          term in section 2.

17          “(2) CYBER THREAT INDICATOR.—The term  
18          ‘cyber threat indicator’ has the meaning given such  
19          term in section 102 of the Cybersecurity Act of  
20          2015.

21          “(3) CYBERSECURITY RISK.—The term ‘cyber-  
22          security risk’ has the meaning given such term in  
23          section 2209.

1           “(4) DIRECTOR.—The term ‘Director’ means  
2 the Director of the Cybersecurity and Infrastructure  
3 Security Agency.

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

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

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

14          “(8) KEY RESOURCES.—The term ‘key re-  
15 sources’ has the meaning given that term in section  
16 2.

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

18               “(A) means each of the several States, the  
19 District of Columbia, and the territories and  
20 possessions of the United States; and

21               “(B) includes any federally recognized In-  
22 dian tribe that notifies the Secretary, not later  
23 than 120 days after the date of the enactment  
24 of this section or not later than 120 days before  
25 the start of any fiscal year in which a grant

1 under this section is awarded, that the tribe in-  
2 tends to develop a Cybersecurity Plan and  
3 agrees to forfeit any distribution under sub-  
4 section (1)(2).”.

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

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

9 **SEC. 3. STRATEGY.**

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

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

18 “(1) IN GENERAL.—Not later than 270 days  
19 after the date of the enactment of this subsection,  
20 the Secretary, acting through the Director, shall, in  
21 coordination with appropriate Federal departments  
22 and agencies, State, local, Tribal, and territorial  
23 governments, the State and Local Cybersecurity Re-  
24 siliance Committee (established under section 2215),  
25 and other stakeholders, as appropriate, develop and

1 make publicly available a Homeland Security Strat-  
2 egy to Improve the Cybersecurity of State, Local,  
3 Tribal, and Territorial Governments that provides  
4 recommendations regarding how the Federal Gov-  
5 ernment should support and promote the ability  
6 State, local, Tribal, and territorial governments to  
7 identify, prepare for, detect, protect against, respond  
8 to, and recover from cybersecurity risks, cybersecu-  
9 rity threats, and incidents (as such term is defined  
10 in section 2209) and establishes baseline require-  
11 ments and principles to which Cybersecurity Plans  
12 under such section shall be aligned.

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

17 “(A) identify capability gaps in the ability  
18 of State, local, Tribal, and territorial govern-  
19 ments to identify, prepare for, detect, protect  
20 against, respond to, and recover from cyberse-  
21 curity risks, cybersecurity threats, and inci-  
22 dents;

23 “(B) identify Federal resources and capa-  
24 bilities that are available or could be made  
25 available to State, local, Tribal, and territorial

1 governments to help such governments identify,  
2 prepare for, detect, protect against, respond to,  
3 and recover from cybersecurity risks, cybersecu-  
4 rity threats, and incidents;

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

13 “(D) identify opportunities to improve the  
14 Agency’s coordination with Federal and non-  
15 Federal entities, such as the Multi-State Infor-  
16 mation Sharing and Analysis Center, to im-  
17 prove incident exercises, information sharing  
18 and incident notification procedures, the ability  
19 for State, local, Tribal, and territorial govern-  
20 ments to voluntarily adapt and implement guid-  
21 ance in Federal binding operational directives,  
22 and opportunities to leverage Federal schedules  
23 for cybersecurity investments under section 502  
24 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           prepare for, detect, protect against, respond to,  
6           and recover from cybersecurity risks, cybersecu-  
7           rity threats, 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, prepare for, detect, pro-  
12          tect against, respond to, and recover from cy-  
13          bersecurity risks, cybersecurity threats, and in-  
14          cidents; and

15          “(G) set dates, including interim bench-  
16          marks, as appropriate for State, local, Tribal,  
17          territorial governments to establish baseline ca-  
18          pabilities to identify, prepare for, detect, protect  
19          against, respond to, and recover from cyberse-  
20          curity risks, cybersecurity threats, and inci-  
21          dents.

22          “(3) CONSIDERATIONS.—In developing the  
23          Homeland Security Strategy to Improve the Cyber-  
24          security of State, Local, Tribal, and Territorial Gov-  
25          ernments required under paragraph (1), the Direc-



1 tor, in coordination with appropriate Federal depart-  
2 ments and agencies, State, local, Tribal, and terri-  
3 torial governments, the State and Local Cybersecu-  
4 rity Resilience Committee, and other stakeholders,  
5 as appropriate, shall consider—

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

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

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

19 “(D) emerging cybersecurity risks to State,  
20 local, Tribal, and territorial governments result-  
21 ing from the deployment of new technologies;  
22 and

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

1 (b) RESPONSIBILITIES OF THE DIRECTOR OF THE  
2 CYBERSECURITY AND INFRASTRUCTURE SECURITY AGEN-  
3 CY.—Subsection (c) of section 2202 of the Homeland Se-  
4 curity Act of 2002 (6 U.S.C. 652) is amended—

5 (1) by redesignating paragraphs (6) through  
6 (11) as paragraphs (10) through (15), respectively;  
7 and

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

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

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

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

○