

# Union Calendar No. 384

116<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

# H. R. 5823

[Report No. 116–478]

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

AUGUST 18, 2020

Additional sponsors: Ms. ESHOO, Ms. SEWELL of Alabama, and Ms. JACKSON LEE

AUGUST 18, 2020

Reported with an amendment; committed to the Committee of the Whole House on the State of the Union and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in *italie*]

[For text of introduced bill, see copy of bill as introduced on February 10, 2020]

# **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 Cyberse-*  
5 *curity Improvement Act”.*

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

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

11 **“SEC. 2215. STATE AND LOCAL CYBERSECURITY GRANT**  
12 **PROGRAM.**

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

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

22 *“(1) The Cybersecurity Plan required under sub-*  
23 *section (d) and approved pursuant to subsection (g).*

24 *“(2) The Homeland Security Strategy to Im-*  
25 *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 Cyberse-*  
4       *curity Grant Program shall be administered in the same*  
5       *program office that administers grants made under sections*  
6       *2003 and 2004.*

7       “(d) *ELIGIBILITY.*—

8               “(1) *IN GENERAL.*—*A State applying for a grant*  
9       *under the State and Local Cybersecurity Grant Pro-*  
10       *gram shall submit to the Secretary a Cybersecurity*  
11       *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, how*  
18       *such State shall—*

19                               “(i) *enhance the preparation, response,*  
20       *and resiliency of information systems*  
21       *owned or operated by such State or, if ap-*  
22       *propriate, by local, Tribal, or territorial*  
23       *governments, against cybersecurity risks*  
24       *and cybersecurity threats;*

1           “(ii) implement a process of contin-  
2           uous cybersecurity vulnerability assessments  
3           and threat mitigation practices prioritized  
4           by degree of risk to address cybersecurity  
5           risks and cybersecurity threats in informa-  
6           tion systems of such State, local, Tribal, or  
7           territorial governments;

8           “(iii) ensure that State, local, Tribal,  
9           and territorial governments that own or op-  
10          erate information systems within the State  
11          adopt best practices and methodologies to  
12          enhance cybersecurity, such as the practices  
13          set forth in the cybersecurity framework de-  
14          veloped by the National Institute of Stand-  
15          ards 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, skills,

1           *and abilities of State, local, Tribal, and ter-*  
2           *ritorial government personnel to address cy-*  
3           *bersecurity risks and cybersecurity threats;*

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

12           *“(vii) assess and mitigate, to the great-*  
13           *est degree possible, cybersecurity risks and*  
14           *cybersecurity threats related to critical in-*  
15           *frastructure and key resources, the degrada-*  
16           *tion of which may impact the performance*  
17           *of information systems within such State;*

18           *“(viii) enhance capability to share*  
19           *cyber threat indicators and related informa-*  
20           *tion between such State and local, Tribal,*  
21           *and territorial governments that own or op-*  
22           *erate information systems within such*  
23           *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 in-  
9   formation 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 deployed  
15                                 on the information systems owned or operated by  
16                                 such State or by local, Tribal, or territorial gov-  
17                                 ernments within such State, including legacy in-  
18                                 formation technology that is no longer supported  
19                                 by the manufacturer.

20                   “(e) *PLANNING COMMITTEES.*—

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

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

4           “(B) *The determination of effective funding*  
5           *priorities for such grant in accordance with sub-*  
6           *section (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, representatives*  
12          *of rural, suburban, and high-population jurisdictions.*

13          “(3) *RULE OF CONSTRUCTION REGARDING EXIST-*  
14          *ING PLANNING COMMITTEES.—Nothing in this sub-*  
15          *section may be construed to require that any State es-*  
16          *tablish a cybersecurity planning committee if such*  
17          *State has established and uses a multijurisdictional*  
18          *planning committee or commission that meets the re-*  
19          *quirements of this paragraph.*

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



1 *ity threats to information systems of State, local, Tribal,*  
2 *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 re-*  
8 *quired under subsection (d).*

9 “(2) *PLAN REQUIREMENTS.*—*In approving a Cy-*  
10 *bersecurity Plan under this subsection, the Director*  
11 *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, com-*  
18 *plies, as appropriate, with the goals and objec-*  
19 *tives of such Strategy.*

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

24 “(4) *EXCEPTION.*—*Notwithstanding the require-*  
25 *ment under subsection (d) to submit a Cybersecurity*

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

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

8 *“(B) such State certifies to the Secretary*  
9 *that the activities that will be supported by such*  
10 *grant are integral to the development of such Cy-*  
11 *bersecurity Plan; or*

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

19 *“(h) LIMITATIONS ON USES OF FUNDS.—*

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

22 *“(A) to supplant State, local, Tribal, or ter-*  
23 *ritorial funds;*

24 *“(B) for any recipient cost-sharing con-*  
25 *tribution;*

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

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

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

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

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

21          “(j) *APPORTIONMENT.*—For fiscal year 2020 and each  
22          fiscal year thereafter, the Secretary shall apportion  
23          amounts appropriated to carry out this section among  
24          States as follows:

1           “(1) *BASELINE AMOUNT.*—*The Secretary shall*  
2 *first apportion 0.25 percent of such amounts to each*  
3 *of American Samoa, the Commonwealth of the North-*  
4 *ern Mariana Islands, Guam, and the Virgin Islands,*  
5 *and 0.75 percent of such amounts to each of the re-*  
6 *maining States.*

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

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

11                   “(B) *the population of all States.*

12           “(k) *FEDERAL SHARE.*—*The Federal share of the cost*  
13 *of an activity carried out using funds made available under*  
14 *the program may not exceed the following percentages:*

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

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

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

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

19                   “(5) *For fiscal year 2025 and each subsequent*  
20 *fiscal year, 50 percent.*

21           “(l) *STATE RESPONSIBILITIES.*—

22                   “(1) *CERTIFICATION.*—*Each State that receives a*  
23 *grant under this section shall certify to the Secretary*  
24 *that the grant will be used for the purpose for which*  
25 *the grant is awarded and in compliance with the Cy-*

1 *bersecurity Plan or other purpose approved by the*  
2 *Secretary under subsection (g).*

3 “(2) *AVAILABILITY OF FUNDS TO LOCAL, TRIBAL,*  
4 *AND TERRITORIAL GOVERNMENTS.—Not later than 45*  
5 *days after a State receives a grant under this section,*  
6 *such State shall, without imposing unreasonable or*  
7 *unduly burdensome requirements as a condition of re-*  
8 *ceipt, obligate or otherwise make available to local,*  
9 *Tribal, and territorial governments in such State,*  
10 *consistent with the applicable Cybersecurity Plan—*

11 “(A) *not less than 80 percent of funds avail-*  
12 *able under such grant;*

13 “(B) *with the consent of such local, Tribal,*  
14 *and territorial governments, items, services, ca-*  
15 *pabilities, or activities having a value of not less*  
16 *than 80 percent of the amount of the grant; or*

17 “(C) *with the consent of the local, Tribal,*  
18 *and territorial governments, grant funds com-*  
19 *bined with other items, services, capabilities, or*  
20 *activities having the total value of not less than*  
21 *80 percent of the amount of the grant.*

22 “(3) *CERTIFICATIONS REGARDING DISTRIBUTION*  
23 *OF GRANT FUNDS TO LOCAL, TRIBAL, TERRITORIAL*  
24 *GOVERNMENTS.—A State shall certify to the Secretary*  
25 *that the State has made the distribution to local,*

1       *Tribal, and territorial governments required under*  
2       *paragraph (2).*

3               “(4) *EXTENSION OF PERIOD.*—*A State may re-*  
4       *quest in writing that the Secretary extend the period*  
5       *of time specified in paragraph (2) for an additional*  
6       *period of time. The Secretary may approve such a re-*  
7       *quest if the Secretary determines such extension is*  
8       *necessary to ensure the obligation and expenditure of*  
9       *grant funds align with the purpose of the grant pro-*  
10       *gram.*

11               “(5) *EXCEPTION.*—*Paragraph (2) shall not*  
12       *apply to the District of Columbia, the Commonwealth*  
13       *of Puerto Rico, American Samoa, the Commonwealth*  
14       *of the Northern Mariana Islands, Guam, or the Vir-*  
15       *gin Islands.*

16               “(6) *DIRECT FUNDING.*—*If a State does not*  
17       *make the distribution to local, Tribal, or territorial*  
18       *governments in such State required under paragraph*  
19       *(2), such a local, Tribal, or territorial government*  
20       *may petition the Secretary.*

21               “(7) *PENALTIES.*—*In addition to other remedies*  
22       *available to the Secretary, the Secretary may termi-*  
23       *nate or reduce the amount of a grant awarded under*  
24       *this section to a State or transfer grant funds pre-*  
25       *viously awarded to such State directly to the appro-*

1        *appropriate local, Tribal, or territorial government if such*  
2        *State violates a requirement of this subsection.*

3        “(m) *ADVISORY COMMITTEE.*—

4                “(1) *ESTABLISHMENT.*—*The Director shall estab-*  
5        *lish a State and Local Cybersecurity Resiliency Com-*  
6        *mittee to provide State, local, Tribal, and territorial*  
7        *stakeholder expertise, situational awareness, and rec-*  
8        *ommendations to the Director, as appropriate, re-*  
9        *garding how to—*

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

13                “(B) *improve the ability of such govern-*  
14        *ments to prevent, protect against, respond, miti-*  
15        *gate, and recover from cybersecurity risks and*  
16        *cybersecurity threats.*

17                “(2) *DUTIES.*—*The State and Local Cybersecu-*  
18        *riety Resiliency Committee shall—*

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

22                “(B) *upon the request of the Director, pro-*  
23        *vide to the Director technical assistance to in-*  
24        *form the review of Cybersecurity Plans submitted*  
25        *by applicants for grants under this section, and,*

1           *as appropriate, submit to the Director rec-*  
2           *ommendations to improve such Plans prior to*  
3           *the Director’s determination regarding whether*  
4           *to approve such Plans;*

5           *“(C) advise and provide to the Director*  
6           *input regarding the Homeland Security Strategy*  
7           *to Improve Cybersecurity for State, Local, Trib-*  
8           *al, and Territorial Governments required under*  
9           *section 2210; and*

10           *“(D) upon the request of the Director, pro-*  
11           *vide to the Director recommendations, as appro-*  
12           *priate, regarding how to—*

13           *“(i) address cybersecurity risks and cy-*  
14           *bersecurity threats on information systems*  
15           *of State, local, Tribal, or territorial govern-*  
16           *ments; and*

17           *“(ii) improve the cybersecurity resil-*  
18           *ience of such governments.*

19           *“(3) MEMBERSHIP.—*

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



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

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

7           “(iii) *One individual recommended to*  
8 *the Director by the National Guard Bureau.*

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

12           “(v) *Two individuals recommended to*  
13 *the Director by the National League of Cit-*  
14 *ies.*

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

18           “(vii) *One individual recommended to*  
19 *the Director by the Multi-State Information*  
20 *Sharing and Analysis Center.*

21           “(viii) *Four individuals who have edu-*  
22 *cational and professional experience related*  
23 *to cybersecurity analysis or policy.*

24           “(B) *TERMS.—Each member of the State*  
25 *and Local Cybersecurity Resiliency Committee*

1           *shall be appointed for a term of two years, except*  
2           *that such term shall be three years only in the*  
3           *case of members who are appointed initially to*  
4           *the Committee upon the establishment of the*  
5           *Committee. Any member appointed to fill a va-*  
6           *cancy occurring before the expiration of the term*  
7           *for which the member's predecessor was ap-*  
8           *pointed shall be appointed only for the remain-*  
9           *der of such term. A member may serve after the*  
10          *expiration of such member's term until a suc-*  
11          *cessor has taken office. A vacancy in the Com-*  
12          *mission shall be filled in the manner in which*  
13          *the original appointment was made.*

14                 “(C) *PAY.—Members of the State and Local*  
15                 *Cybersecurity Resiliency Committee shall serve*  
16                 *without pay.*

17                 “(4) *CHAIRPERSON; VICE CHAIRPERSON.—The*  
18                 *members of the State and Local Cybersecurity Resil-*  
19                 *iency Committee shall select a chairperson and vice*  
20                 *chairperson from among Committee members.*

21                 “(5) *FEDERAL ADVISORY COMMITTEE ACT.—The*  
22                 *Federal Advisory Committee Act (5 U.S.C. App.)*  
23                 *shall not apply to the State and Local Cybersecurity*  
24                 *Resilience Committee.*

25                 “(n) *REPORTS.—*

1           “(1) *ANNUAL REPORTS BY STATE GRANT RECIPI-*  
2           *ENTS.—A State that receives a grant under this sec-*  
3           *tion shall annually submit to the Secretary a report*  
4           *on the progress of the State in implementing the Cy-*  
5           *bersecurity Plan approved pursuant to subsection (g).*  
6           *If the State does not have a Cybersecurity Plan ap-*  
7           *proved pursuant to subsection (g), the State shall sub-*  
8           *mit to the Secretary a report describing how grant*  
9           *funds were obligated and expended to develop a Cy-*  
10           *bersecurity Plan or improve the cybersecurity of in-*  
11           *formation systems owned or operated by State, local,*  
12           *Tribal, or territorial governments in such State. The*  
13           *Secretary, acting through the Director, shall make*  
14           *each such report publicly available, including by*  
15           *making each such report available on the internet*  
16           *website of the Agency, subject to any redactions the*  
17           *Director determines necessary to protect classified or*  
18           *other sensitive information.*

19           “(2) *ANNUAL REPORTS TO CONGRESS.—At least*  
20           *once each year, the Secretary, acting through the Di-*  
21           *rector, shall submit to Congress a report on the use*  
22           *of grants awarded under this section and any*  
23           *progress made toward the following:*

24                           “(A) *Achieving the objectives set forth in the*  
25                           *Homeland Security Strategy to Improve the Cy-*

1           *bersecurity of State, Local, Tribal, and Terri-*  
2           *torial Governments, upon the strategy’s issuance*  
3           *under section 2210.*

4           “(B) *Developing, implementing, or revising*  
5           *Cybersecurity Plans.*

6           “(C) *Reducing cybersecurity risks and cy-*  
7           *bersecurity threats to information systems owned*  
8           *or operated by State, local, Tribal, and terri-*  
9           *torial governments as a result of the award of*  
10          *such grants.*

11          “(o) *AUTHORIZATION OF APPROPRIATIONS.—There*  
12          *are authorized to be appropriated for grants under this sec-*  
13          *tion—*

14                 “(1) *for each of fiscal years 2021 through 2025,*  
15                 *\$400,000,000; and*

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

18          “(p) *DEFINITIONS.—In this section:*

19                 “(1) *CRITICAL INFRASTRUCTURE.—The term*  
20                 *‘critical infrastructure’ has the meaning given that*  
21                 *term in section 2.*

22                 “(2) *CYBER THREAT INDICATOR.—The term*  
23                 *‘cyber threat indicator’ has the meaning given such*  
24                 *term in section 102 of the Cybersecurity Act of 2015.*

1           “(3) *DIRECTOR*.—The term ‘Director’ means the  
2           *Director of the Cybersecurity and Infrastructure Se-*  
3           *curity Agency.*

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

6           “(5) *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          “(6) *INFORMATION SYSTEM*.—The term ‘informa-  
11          *tion system’ has the meaning given such term in sec-*  
12          *tion 102(9) of the Cybersecurity Act of 2015 (6 U.S.C.*  
13          *1501(9)).*

14          “(7) *KEY RESOURCES*.—The term ‘key resources’  
15          *has the meaning given that term in section 2.*

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

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

21                 “(A) *means each of the several States, the*  
22                 *District of Colombia, and the territories and pos-*  
23                 *sessions of the United States; and*

24                 “(B) *includes any federally recognized In-*  
25                 *dian tribe that notifies the Secretary, not later*

1           *than 120 days after the date of the enactment of*  
 2           *this section or not later than 120 days before the*  
 3           *start of any fiscal year in which a grant under*  
 4           *this section is awarded, that the tribe intends to*  
 5           *develop a Cybersecurity Plan and agrees to for-*  
 6           *feit any distribution under subsection (l)(2).*

7   **“SEC. 2216. CYBERSECURITY RESOURCE GUIDE DEVELOP-**  
 8                   **MENT FOR STATE, LOCAL, TRIBAL, AND TER-**  
 9                   **RITORIAL GOVERNMENT OFFICIALS.**

10           *“The Secretary, acting through the Director, shall de-*  
 11           *velop a resource guide for use by State, local, Tribal, and*  
 12           *territorial government officials, including law enforcement*  
 13           *officers, to help such officials identify, prepare for, detect,*  
 14           *protect against, respond to, and recover from cybersecurity*  
 15           *risks, cybersecurity threats, and incidents (as such term is*  
 16           *defined in section 2209).”.*

17           *(b) CLERICAL AMENDMENT.—The table of contents in*  
 18           *section 1(b) of the Homeland Security Act of 2002 is*  
 19           *amended by inserting after the item relating to section 2214*  
 20           *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.”.*

21   **SEC. 3. STRATEGY.**

22           *(a) HOMELAND SECURITY STRATEGY TO IMPROVE*  
 23           *THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TER-*  
 24           *RITORIAL GOVERNMENTS.—Section 2210 of the Homeland*

1 *Security Act of 2002 (6 U.S.C. 660) is amended by adding*  
2 *at the end the following new subsection:*

3       “(e) *HOMELAND SECURITY STRATEGY TO IMPROVE*  
4 *THE CYBERSECURITY OF STATE, LOCAL, TRIBAL, AND TER-*  
5 *RITORIAL GOVERNMENTS.—*

6               “(1) *IN GENERAL.—Not later than 270 days*  
7 *after the date of the enactment of this subsection, the*  
8 *Secretary, acting through the Director, shall, in co-*  
9 *ordination with appropriate Federal departments and*  
10 *agencies, State, local, Tribal, and territorial govern-*  
11 *ments, the State and Local Cybersecurity Resilience*  
12 *Committee (established under section 2215), and other*  
13 *stakeholders, as appropriate, develop and make pub-*  
14 *licly available a Homeland Security Strategy to Im-*  
15 *prove the Cybersecurity of State, Local, Tribal, and*  
16 *Territorial Governments that provides recommenda-*  
17 *tions regarding how the Federal Government should*  
18 *support and promote the ability State, local, Tribal,*  
19 *and territorial governments to identify, protect*  
20 *against, detect respond to, and recover from cyberse-*  
21 *curity risks, cybersecurity threats, and incidents (as*  
22 *such term is defined in section 2209) and establishes*  
23 *baseline requirements and principles to which Cyber-*  
24 *security Plans under such section shall be aligned.*

1           “(2) CONTENTS.—*The Homeland Security Strat-*  
2           *egy to Improve the Cybersecurity of State, Local,*  
3           *Tribal, and Territorial Governments required under*  
4           *paragraph (1) shall—*

5                   “(A) *identify capability gaps in the ability*  
6                   *of State, local, Tribal, and territorial govern-*  
7                   *ments to identify, protect against, detect, respond*  
8                   *to, and recover from cybersecurity risks, cyberse-*  
9                   *curity threats, and incidents;*

10                   “(B) *identify Federal resources and capa-*  
11                   *bilities that are available or could be made*  
12                   *available to State, local, Tribal, and territorial*  
13                   *governments to help such governments identify,*  
14                   *protect against, detect, respond to, and recover*  
15                   *from cybersecurity risks, cybersecurity threats,*  
16                   *and incidents;*

17                   “(C) *identify and assess the limitations of*  
18                   *Federal resources and capabilities available to*  
19                   *State, local, Tribal, and territorial governments*  
20                   *to help such governments identify, protect*  
21                   *against, detect, respond to, and recover from cy-*  
22                   *bersecurity risks, cybersecurity threats, and inci-*  
23                   *dents, and make recommendations to address*  
24                   *such limitations;*



1           “(D) identify opportunities to improve the  
2           Agency’s coordination with Federal and non-  
3           Federal entities, such as the Multi-State Infor-  
4           mation Sharing and Analysis Center, to improve  
5           incident exercises, information sharing and inci-  
6           dent notification procedures, the ability for  
7           State, local, Tribal, and territorial governments  
8           to voluntarily adapt and implement guidance in  
9           Federal binding operational directives, and op-  
10          portunities to leverage Federal schedules for cy-  
11          bersecurity investments under section 502 of title  
12          40, United States Code;

13          “(E) recommend new initiatives the Federal  
14          Government should undertake to improve the  
15          ability of State, local, Tribal, and territorial  
16          governments to help such governments identify,  
17          protect against, detect, respond to, and recover  
18          from cybersecurity risks, cybersecurity threats,  
19          and incidents;

20          “(F) set short-term and long-term goals that  
21          will improve the ability of State, local, Tribal,  
22          and territorial governments to help such govern-  
23          ments identify, protect against, detect, respond  
24          to, and recover from cybersecurity risks, cyberse-  
25          curity threats, and incidents; and

1           “(G) set dates, including interim bench-  
2           marks, as appropriate for State, local, Tribal,  
3           territorial governments to establish baseline ca-  
4           pabilities to identify, protect against, detect, re-  
5           spond to, and recover from cybersecurity risks,  
6           cybersecurity threats, and incidents.

7           “(3) CONSIDERATIONS.—In developing the  
8           Homeland Security Strategy to Improve the Cyberse-  
9           curity of State, Local, Tribal, and Territorial Gov-  
10          ernments required under paragraph (1), the Director,  
11          in coordination with appropriate Federal depart-  
12          ments and agencies, State, local, Tribal, and terri-  
13          torial governments, the State and Local Cybersecurity  
14          Resilience Committee, and other stakeholders, as ap-  
15          propriate, shall consider—

16           “(A) lessons learned from incidents that  
17           have affected State, local, Tribal, and territorial  
18           governments, and exercises with Federal and  
19           non-Federal entities;

20           “(B) the impact of incidents that have af-  
21           fected State, local, Tribal, and territorial govern-  
22           ments, including the resulting costs to such gov-  
23           ernments;

24           “(C) the information related to the interest  
25           and ability of state and non-state threat actors

1           to compromise information systems owned or op-  
2           erated by State, local, Tribal, and territorial  
3           governments;

4                   “(D) emerging cybersecurity risks and cy-  
5           bersecurity threats to State, local, Tribal, and  
6           territorial governments resulting from the de-  
7           ployment of new technologies; and

8                   “(E) recommendations made by the State  
9           and Local Cybersecurity Resilience Committee.”.

10           (b) *RESPONSIBILITIES OF THE DIRECTOR OF THE CY-*  
11 *BERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—*  
12 *Subsection (c) of section 2202 of the Homeland Security*  
13 *Act of 2002 (6 U.S.C. 652) is amended—*

14                   (1) *by redesignating paragraphs (6) through (11)*  
15 *as paragraphs (11) through (16), respectively; and*

16                   (2) *by inserting after paragraph (5) the fol-*  
17 *lowing new paragraphs:*

18                   “(6) *develop program guidance, in consultation*  
19 *with the State and Local Government Cybersecurity*  
20 *Resiliency Committee established under section 2215,*  
21 *for the State and Local Cybersecurity Grant Program*  
22 *under such section or any other homeland security as-*  
23 *sistance administered by the Department to improve*  
24 *cybersecurity;*

1           “(7) review, in consultation with the State and  
2           *Local Cybersecurity Resiliency Committee, all cyber-*  
3           *security plans of State, local, Tribal, and territorial*  
4           *governments developed pursuant to any homeland se-*  
5           *curity assistance administered by the Department to*  
6           *improve cybersecurity;*

7           “(8) provide expertise and technical assistance to  
8           *State, local, Tribal, and territorial government offi-*  
9           *cial with respect to cybersecurity;*

10           “(9) provide education, training, and capacity  
11           *development to enhance the security and resilience of*  
12           *cybersecurity and infrastructure security;*

13           “(10) provide information to State, local, Tribal,  
14           *and territorial governments on the security benefits of*  
15           *.gov domain name registration services;”.*

16           (c) *FEASIBILITY STUDY.*—Not later than 180 days  
17           *after the date of the enactment of this Act, the Director of*  
18           *the Cybersecurity and Infrastructure Security Agency of the*  
19           *Department of Homeland Security shall conduct a study*  
20           *to assess the feasibility of implementing a short-term rota-*  
21           *tional program for the detail of approved State, local, Trib-*  
22           *al, and territorial government employees in cyber workforce*  
23           *positions to the Agency.*



Union Calendar No. 384

116<sup>TH</sup> CONGRESS  
2<sup>D</sup> SESSION

**H. R. 5823**

[Report No. 116-478]

---

---

## **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.

---

---

AUGUST 18, 2020

Reported with an amendment; committed to the Committee of the Whole House on the State of the Union and ordered to be printed