

116TH CONGRESS
2D SESSION

H. R. 8048

To establish in the Department of Homeland Security a program to make grants for emergency information technology expenses, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

AUGUST 14, 2020

Mr. LANGEVIN (for himself, Mr. GALLAGHER, Mr. RUPPERSBERGER, Mr. HURD of Texas, Mr. RICHMOND, Mr. McCAUL, Mr. ROSE of New York, and Mr. BACON) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Oversight and Reform, and Energy and Commerce, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To establish in the Department of Homeland Security a program to make grants for emergency information technology expenses, 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 IT
5 Modernization and Cybersecurity Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

1 (1) AGENCY.—The term “Agency” means the
2 Cybersecurity and Infrastructure Security Agency of
3 the Department of Homeland Security.

4 (2) APPROPRIATE CONGRESSIONAL COMMIT-
5 TEES.—The term “appropriate congressional com-
6 mittees” means—

7 (A) the Committee on Homeland Security
8 and Governmental Affairs of the Senate; and

9 (B) the Committee on Homeland Security
10 of the House of Representatives.

11 (3) COVERED INFORMATION TECHNOLOGY.—In
12 this section, the term “covered information tech-
13 nology” includes the following information tech-
14 nology:

15 (A) Enterprise productivity tools, includ-
16 ing—

17 (i) email services;

18 (ii) computer software for the pur-
19 poses of managing payroll and budget;

20 (iii) personnel management solutions;

21 and

22 (iv) customer relationship manage-
23 ment software relating to the provision of
24 services to users of such services.

25 (B) Cybersecurity services and tools.

1 (C) Computer networking equipment.

2 (4) COVERED INFORMATION TECHNOLOGY
3 SERVICES.—The term “covered information tech-
4 nology services” means any service necessary to in-
5 stall, implement, maintain, or upgrade covered infor-
6 mation technology.

7 (5) DEPARTMENT.—The term “Department”
8 means the Department of Homeland Security.

9 (6) DIRECTOR.—The term “Director” means
10 the Director of the Cybersecurity and Infrastructure
11 Security Agency of the Department of Homeland Se-
12 curity.

13 (7) EMERGENCY INFORMATION TECHNOLOGY
14 EXPENSES.—The term “emergency information
15 technology expenses” means expenses related to—

16 (A) improving covered information tech-
17 nology;

18 (B) conducting covered information tech-
19 nology services;

20 (C) subsidizing payroll for information
21 technology staff to maintain the current staff-
22 ing level; or

23 (D) government employees having the nec-
24 essary covered information technology to
25 telework.

1 (8) FISCAL YEAR.—The term “fiscal year” has
2 the meaning given the term under the State or local
3 law of the relevant grant recipient.

4 (9) INFORMATION TECHNOLOGY.—The term
5 “information technology” has the meaning given the
6 term in section 11101 of title 40, United States
7 Code.

8 (10) PUBLIC HEALTH EMERGENCY.—The term
9 “public health emergency” means the public health
10 emergency declared by the Secretary of Health and
11 Human Services pursuant to section 319 of the Pub-
12 lic Health Service Act (42 U.S.C. 247d) on January
13 31, 2020, with respect to COVID–19.

14 (11) SECRETARY.—The term “Secretary”
15 means the Secretary of Homeland Security.

16 (12) STATE.—The term “State” has the mean-
17 ing given the term in section 311 of title 5, United
18 States Code.

19 (13) TRIBAL GOVERNMENT.—The term “Tribal
20 government” has the meaning given the term in sec-
21 tion 421(13) of the Congressional Budget and Im-
22 poundment Control Act of 1974 (2 U.S.C. 658(13)).

1 **SEC. 3. PUBLIC HEALTH EMERGENCY INFORMATION TECH-**
2 **NOLOGY GRANT PROGRAM.**

3 (a) ESTABLISHMENT.—There is established in the
4 Department a program to be known as the “Public Health
5 Emergency Information Technology Grant Program” (in
6 this section referred to as the “Public Health Emergency
7 IT Grant Program”), under which the Secretary may
8 award grants to States for emergency information tech-
9 nology expenses during the public health emergency.

10 (b) APPLICATION.—Each State may apply for a grant
11 under the Public Health Emergency IT Grant Program,
12 and shall submit such information in support of such a
13 grant as the Secretary may require.

14 (c) ALLOCATION OF FUNDS.—

15 (1) TRIBAL GOVERNMENTS.—Grants to Tribal
16 governments under the Public Health Emergency IT
17 Grant Program may not exceed \$25,000,000 in the
18 aggregate.

19 (2) ADMINISTRATION AND OVERSIGHT.—The
20 Secretary may not expend more than \$10,000,000
21 for administration of the Public Health Emergency
22 IT Grant Program.

23 (d) CONDITIONS ON RECEIPT OF GRANT.—

24 (1) MANAGEMENT OF FUNDS.—To be eligible
25 for a grant under the Public Health Emergency IT
26 Grant Program, a State shall agree to designate the

1 Chief Information Officer, or an equivalent official,
2 of the State as the primary official for the manage-
3 ment and allocation of funds awarded under the
4 Public Health Emergency IT Grant Program.

5 (2) SECURITY STANDARDS AND CERTIFI-
6 CATIONS.—

7 (A) IN GENERAL.—Not later than 90 days
8 after the date of the enactment of this Act, the
9 Secretary, in consultation with the Secretary of
10 Commerce, shall select commonly accepted secu-
11 rity standards and certifications with respect to
12 covered information technology.

13 (B) SECURITY STANDARDS AND CERTIFI-
14 CATIONS REQUIRED.—To be eligible for a grant
15 under the Public Health Emergency IT Grant
16 Program, a State shall agree to procure only
17 covered information technology that meets or
18 exceeds the standards and certifications selected
19 pursuant to paragraph (1) with funds made
20 available under such Program.

21 (e) GRANTS.—

22 (1) SINGLE GRANT.—A State may not receive
23 more than one grant under the Public Health Emer-
24 gency IT Grant Program.

1 (2) GRANT AMOUNTS.—The Secretary may
2 award grants to States under the Public Health
3 Emergency IT Grant Program on the basis of the
4 population of such State, except no grant awarded
5 under such Program may be less than \$5,000,000.

6 (f) SUBGRANTS.—Each State that receives a grant
7 under the Public Health Emergency IT Grant Program
8 shall reserve not less than 40 percent of amounts received
9 for the purpose of making subgrants to local governments
10 within such State—

11 (1) for emergency information technology ex-
12 penses; or

13 (2) to purchase licenses for covered information
14 technology on behalf of such local governments.

15 (g) RETURN OF FUNDS.—Amounts received by
16 States under the Public Health Emergency IT Grant Pro-
17 gram that are not expended by the date that is two years
18 after the date of the receipt of such funds shall be re-
19 turned to the Treasury of the United States.

20 (h) REPORTS.—

21 (1) REPORTS BY GRANT RECIPIENTS.—Not
22 later than 180 days after receiving a grant under
23 the Public Health Emergency IT Grant Program, a
24 recipient of such grant shall submit to the Secretary
25 a report that—

1 (A) describes how grant funds were obli-
2 gated or expended, including the use of funds
3 made available as subgrants; and

4 (B) demonstrates compliance by such re-
5 cipient and subgrantee with the requirements of
6 such Program.

7 (2) ANNUAL REPORT TO CONGRESS.—Not later
8 than 1 year after the date of the enactment of this
9 Act and annually thereafter until all funds under the
10 Public Health Emergency IT Grant Program are ex-
11 pended or returned to the Treasury of the United
12 States, the Secretary shall submit to the appropriate
13 congressional committees a report that—

14 (A) describes how grant funds were obli-
15 gated or expended, including the use of funds
16 made available as subgrants; and

17 (B) demonstrates compliance by each re-
18 cipient and subgrantee with the requirements of
19 such Program.

20 (i) AUTHORIZATION OF APPROPRIATIONS.—There is
21 authorized to be appropriated \$1,000,000,000 for grants
22 under the Public Health Emergency IT Grant Program.
23 Amounts authorized to be appropriated pursuant to this
24 subsection are authorized to remain available until Sep-
25 tember 30, 2022.

1 **SEC. 4. MODERNIZING IT GRANT PROGRAM.**

2 (a) ESTABLISHMENT.—There is established in the
3 Department a program to be known as the “Modernizing
4 IT Grant Program”, under which the Secretary may make
5 grants to States to modernize information technology for
6 the purpose of securely enabling digital delivery of govern-
7 ment services, including the digital delivery of—

8 (1) emergency services;

9 (2) government benefit and entitlement pro-
10 grams; and

11 (3) administrative services performed by a
12 State.

13 (b) ELIGIBILITY.—To be eligible for a grant under
14 the Modernizing IT Grant Program, a State shall—

15 (1) with respect to fiscal years 2021, 2022, and
16 2023, maintain the funding levels of the lesser of fis-
17 cal year 2019, or the average of fiscal years 2017,
18 2018, and 2019, with respect to information tech-
19 nology support and modernization; and

20 (2) provide matching funds equal to 5 percent
21 of the amount of any grant received under the Mod-
22 ernizing IT Grant Program.

23 (c) APPLICATION.—

24 (1) IN GENERAL.—Each State may apply for a
25 grant under the Modernizing IT Grant Program,
26 and shall submit such information in support of

1 such a grant as the Secretary may require, including
2 the following:

3 (A) A State information technology mod-
4 ernization plan, including—

5 (i) a description of existing informa-
6 tion technology;

7 (ii) the costs related to maintenance
8 of existing information technology;

9 (iii) a compilation of recent security
10 audits of existing information technology;

11 (iv) a compilation of recent oper-
12 ational performance reports of existing in-
13 formation technology;

14 (v) a methodology to prioritize
15 projects and procurement to account for—

16 (I) security gains;

17 (II) operational gains; and

18 (III) cost; and

19 (vi) a transition plan to modernize ex-
20 isting information technology, including—

21 (I) a comparative analysis of
22 cloud-based versus on-premise solu-
23 tions; and

24 (II) an estimate of operation and
25 maintenance costs for the information

1 technology to be procured under such
2 transition plan.

3 (B) A local government information tech-
4 nology modernization plan describing how
5 grants awarded under the Modernizing IT
6 Grant Program will be used to provide—

7 (i) subgrants to local governments to
8 modernize their information technology
9 supporting digital delivery of government
10 services; or

11 (ii) shared services to local govern-
12 ments to support the digital delivery of
13 government services.

14 (2) APPLICATION EVALUATION.—The Sec-
15 retary, acting through the Director, and in consulta-
16 tion with the Administrator of General Services,
17 shall evaluate each application for a grant under the
18 Modernizing IT Grant Program with respect to the
19 appropriateness of the information technology mod-
20 ernization plan to improve cybersecurity and en-
21 hance the capability to effectively deliver digital gov-
22 ernment services.

23 (3) TECHNICAL ASSISTANCE.—The Director
24 may provide technical assistance to States applying
25 for a grant under the Modernizing IT Grant Pro-

1 gram with respect to State and local government in-
2 formation technology modernization plans described
3 in paragraph (1)(B).

4 (d) CONDITIONS ON RECEIPT OF GRANT.—

5 (1) MANAGEMENT OF FUNDS.—To be eligible
6 for a grant under the Modernizing IT Grant Pro-
7 gram, a State shall agree to designate the Chief In-
8 formation Officer, or an equivalent official, of the
9 State as the primary official for the management
10 and allocation of funds awarded under the Modern-
11 izing IT Grant Program.

12 (2) SECURITY STANDARDS AND CERTIFI-
13 CATIONS.—

14 (A) IN GENERAL.—Not later than 1 year
15 after the date of the enactment of this Act, the
16 Secretary, in consultation with the Secretary of
17 Commerce, shall select commonly accepted secu-
18 rity standards and certifications with respect to
19 information technology.

20 (B) SECURITY STANDARDS AND CERTIFI-
21 CATIONS REQUIRED.—To be eligible for a grant
22 under the Modernizing IT Grant Program, a
23 State shall agree to procure only information
24 technology that meets or exceeds the standards

1 and certifications described in paragraph (1)
2 with funds made available under such Program.

3 (e) GRANTS.—

4 (1) SINGLE GRANT.—A State may not receive
5 more than one grant under the Modernizing IT
6 Grant Program.

7 (2) GRANT AMOUNTS.—

8 (A) STATE GOVERNMENTS.—The Secretary
9 may determine the amount of a grant to be
10 awarded to a State, excluding Tribal govern-
11 ments, under the Modernizing IT Grant Pro-
12 gram based on the population of such State, ex-
13 cept no grant awarded under such Program
14 may be less than \$100,000,000.

15 (B) TRIBAL GOVERNMENTS.—Grants to
16 Tribal governments under the Modernization
17 Grant Program may not exceed \$500,000,000
18 in the aggregate.

19 (3) DISBURSEMENT OF FUNDS.—Grant funds
20 awarded under the Modernizing IT Grant Program
21 shall be dispersed in structured payments over a pe-
22 riod of five years, in such increments as the Sec-
23 retary determines appropriate for the project or pro-
24 curement to be carried out using the funds.

1 (f) SUBGRANTS.—Each State that receives a grant
2 under the Modernizing IT Grant Program shall reserve
3 not less than 40 percent of amounts received under such
4 grant for the purpose of making a subgrant to local gov-
5 ernments to implement the local government information
6 technology modernization plan required under subsection
7 (c)(1)(B).

8 (g) RETURN OF FUNDS.—Amounts received under
9 the Modernizing IT Grant Program that are not expended
10 by the date that is five years after the date of the receipt
11 of such funds shall be returned to the Treasury of the
12 United States.

13 (h) ADMINISTRATIVE COSTS.—The Secretary may
14 not expend more than \$25,000,000 for administration of
15 the Modernizing IT Grant Program.

16 (i) REPORTS.—

17 (1) REPORTS BY GRANT RECIPIENTS.—Not
18 later than 180 days after receiving a grant under
19 the Modernizing IT Grant Program, a recipient of
20 such grant shall submit to the Secretary a report
21 that—

22 (A) describes how grant funds were obli-
23 gated or expended, including the use of funds
24 made available as subgrants; and

1 (B) demonstrates compliance by each re-
2 cipient and subgrantee with the requirements of
3 such Program.

4 (2) ANNUAL REPORT TO CONGRESS.—Not later
5 than 1 year after the date of the first grant awarded
6 under the Modernizing IT Grant Program and an-
7 nually thereafter until all funds are expended or re-
8 turned to the Treasury of the United States, the
9 Secretary shall submit to the appropriate congres-
10 sional committees a report that—

11 (A) describes how grant funds were obli-
12 gated or expended, including the use of funds
13 made available as subgrants; and

14 (B) demonstrates compliance by each re-
15 cipient and subgrantee with the requirements of
16 such Program.

17 (j) AUTHORIZATION OF APPROPRIATIONS.—There is
18 authorized to be appropriated \$25,000,000,000 for grants
19 under the Modernizing IT Grant Program. Amounts au-
20 thorized to be appropriated pursuant to this subsection are
21 authorized to remain available until September 30, 2027.

22 **SEC. 5. STATE AND LOCAL CYBERSECURITY GRANT PRO-**
23 **GRAM.**

24 (a) IN GENERAL.—Subtitle A of title XXII of the
25 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)

1 is amended by adding at the end the following new sec-
2 tions:

3 **“SEC. 2215. STATE AND LOCAL CYBERSECURITY GRANT**
4 **PROGRAM.**

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

12 “(b) BASELINE REQUIREMENTS.—A grant awarded
13 under this section shall be used in compliance with the
14 following:

15 “(1) The Cybersecurity Plan required under
16 subsection (d) and approved pursuant to subsection
17 (g).

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

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

1 “(d) ELIGIBILITY.—

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

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

11 “(B) describe, to the extent practicable,
12 how such State shall—

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

19 “(ii) implement a process of contin-
20 uous cybersecurity vulnerability assess-
21 ments and threat mitigation practices
22 prioritized by degree of risk to address cy-
23 bersecurity risks and cybersecurity threats
24 in information systems of such State, local,
25 Tribal, or territorial governments;

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

9 “(iv) promote the delivery of safe, rec-
10 ognizable, and trustworthy online services
11 by State, local, Tribal, and territorial gov-
12 ernments, including through the use of the
13 .gov internet domain;

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

23 “(vi) ensure continuity of communica-
24 tions and data networks within such State
25 between such State and local, Tribal, and

1 territorial governments that own or operate
2 information systems within such State in
3 the event of an incident involving such
4 communications or data networks within
5 such State;

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

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

19 “(ix) develop and coordinate strategies
20 to address cybersecurity risks and cyberse-
21 curity threats in consultation with—

22 “(I) local, Tribal, and territorial
23 governments within the State; and

24 “(II) as applicable—

1 “(aa) neighboring States or,
2 as appropriate, members of an
3 information sharing and analysis
4 organization; and

5 “(bb) neighboring countries;
6 and

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

14 “(2) DISCRETIONARY ELEMENTS.—The Cyber-
15 security Plan of a State described in paragraph (1)
16 may include—

17 “(A) cooperative programs developed by
18 groups of local, Tribal, and territorial govern-
19 ments within such State to address cybersecu-
20 rity risks and cybersecurity threats; and

21 “(B) programs provided by such State to
22 support local, Tribal, and territorial govern-
23 ments and critical infrastructure owners and
24 operators to address cybersecurity risks and cy-
25 bersecurity threats.

1 “(e) PLANNING COMMITTEES.—

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

5 “(A) The development, implementation,
6 and revision of such State’s Cybersecurity Plan
7 required under subsection (d).

8 “(B) The determination of effective fund-
9 ing priorities for such grant in accordance with
10 subsection (f).

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

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

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

8 “(g) APPROVAL OF PLANS.—

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

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

17 “(A) meets the requirements specified in
18 subsection (d); and

19 “(B) upon issuance of the Homeland Secu-
20 rity Strategy to Improve the Cybersecurity of
21 State, Local, Tribal, and Territorial Govern-
22 ments authorized pursuant to section 2210,
23 complies, as appropriate, with the goals and ob-
24 jectives of such Strategy.

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

5 “(4) EXCEPTION.—Notwithstanding the re-
6 quirement under subsection (d) to submit a Cyberse-
7 curity Plan as a condition of apply for a grant under
8 this section, such a grant may be awarded to a State
9 that has not so submitted a Cybersecurity Plan to
10 the Secretary if—

11 “(A) such State certifies to the Secretary
12 that it will submit to the Secretary a Cyberse-
13 curity Plan for approval by September 30,
14 2022;

15 “(B) such State certifies to the Secretary
16 that the activities that will be supported by
17 such grant are integral to the development of
18 such Cybersecurity Plan; or

19 “(C) such State certifies to the Secretary,
20 and the Director confirms, that the activities
21 that will be supported by the grant will address
22 imminent cybersecurity risks or cybersecurity
23 threats to the information systems of such
24 State or of a local, Tribal, or territorial govern-
25 ment in such State.

1 “(h) LIMITATIONS ON USES OF FUNDS.—

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

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

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

8 “(C) to pay a demand for ransom in an at-
9 tempt to regain access to information or an in-
10 formation system of such State or of a local,
11 Tribal, or territorial government in such State;

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

13 “(E) for any purpose that does not directly
14 address cybersecurity risks or cybersecurity
15 threats on an information systems of such State
16 or of a local, Tribal, or territorial government
17 in such State.

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

23 “(i) OPPORTUNITY TO AMEND APPLICATIONS.—In
24 considering applications for grants under this section, the
25 Secretary shall provide applicants with a reasonable op-

1 portunity to correct defects, if any, in such applications
2 before making final awards.

3 “(j) APPORTIONMENT.—For fiscal year 2020 and
4 each fiscal year thereafter, the Secretary shall apportion
5 amounts appropriated to carry out this section among
6 States as follows:

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

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

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

17 “(B) the population of all States.

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

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

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

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

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

1 “(5) For fiscal year 2025 and each subsequent
2 fiscal year, 50 percent.

3 “(1) STATE RESPONSIBILITIES.—

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

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

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

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

1 “(C) with the consent of the local, Tribal,
2 and territorial governments, grant funds com-
3 bined with other items, services, capabilities, or
4 activities having the total value of not less than
5 80 percent of the amount of the grant.

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

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

20 “(5) EXCEPTION.—Paragraph (2) shall not
21 apply to the District of Columbia, the Common-
22 wealth of Puerto Rico, American Samoa, the Com-
23 monwealth of the Northern Mariana Islands, Guam,
24 or the Virgin Islands.

1 “(6) DIRECT FUNDING.—If a State does not
2 make the distribution to local, Tribal, or territorial
3 governments in such State required under paragraph
4 (2), such a local, Tribal, or territorial government
5 may petition the Secretary.

6 “(7) PENALTIES.—In addition to other rem-
7 edies available to the Secretary, the Secretary may
8 terminate or reduce the amount of a grant awarded
9 under this section to a State or transfer grant funds
10 previously awarded to such State directly to the ap-
11 propriate local, Tribal, or territorial government if
12 such State violates a requirement of this subsection.

13 “(m) ADVISORY COMMITTEE.—

14 “(1) ESTABLISHMENT.—The Director shall es-
15 tablish a State and Local Cybersecurity Resiliency
16 Committee to provide State, local, Tribal, and terri-
17 torial stakeholder expertise, situational awareness,
18 and recommendations to the Director, as appro-
19 priate, regarding how to—

20 “(A) address cybersecurity risks and cyber-
21 security threats to information systems of
22 State, local, Tribal, or territorial governments;
23 and

24 “(B) improve the ability of such govern-
25 ments to prevent, protect against, respond,

1 mitigate, and recover from cybersecurity risks
2 and cybersecurity threats.

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

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

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

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

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

24 “(i) address cybersecurity risks and
25 cybersecurity threats on information sys-

1 tems of State, local, Tribal, or territorial
2 governments; and

3 “(ii) improve the cybersecurity resil-
4 ience of such governments.

5 “(3) MEMBERSHIP.—

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

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

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

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

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

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

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

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

7 “(viii) Four individuals who have edu-
8 cational and professional experience related
9 to cybersecurity analysis or policy.

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

1 “(C) PAY.—Members of the State and
2 Local Cybersecurity Resiliency Committee shall
3 serve without pay.

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

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

12 “(n) REPORTS.—

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

1 tor, shall make each such report publicly available,
2 including by making each such report available on
3 the internet website of the Agency, subject to any
4 redactions the Director determines necessary to pro-
5 tect classified or other sensitive information.

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

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

16 “(B) Developing, implementing, or revising
17 Cybersecurity Plans.

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

23 “(o) AUTHORIZATION OF APPROPRIATIONS.—There
24 are authorized to be appropriated for grants under this
25 section—

1 “(1) for each of fiscal years 2021 through
2 2025, \$400,000,000; and

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

5 “(p) DEFINITIONS.—In this section:

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

9 “(2) CYBER THREAT INDICATOR.—The term
10 ‘cyber threat indicator’ has the meaning given such
11 term in section 102 of the Cybersecurity Act of
12 2015.

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

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

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

22 “(6) INFORMATION SYSTEM.—The term ‘infor-
23 mation system’ has the meaning given such term in
24 section 102(9) of the Cybersecurity Act of 2015 (6
25 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 Columbia, 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 (1)(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. 6. 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 territorial 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 shall conduct a study to assess the feasibility of imple-
10 menting a short-term rotational program for the detail of
11 approved State, local, Tribal, and territorial government
12 employees in cyber workforce positions to the Agency.

○