SB0120

CONGRESS.GOV

H.R.5823 - State and Local Cybersecurity Improvement Act

116th Congress (2019-2020) | Get alerts

Sponsor: Rep. Richmond, Cedric L. [D-LA-2] (Introduced 02/10/2020)
Committees: House - Homeland Security
Latest Action: House - 02/10/2020 Referred to the House Committee on Homeland Security. (All Actions)
Tracker: **Introduced** Passed House Passed Senate To President Became Law

Summary(0) **Text(1)** Actions(2) Titles(2) Amendments(0) Cosponsors(14) Committees(1) Related Bills(0)

There is one version of the bill.

Text available as: XML/HTML | XML/HTML (new window) | TXT | PDF (PDF provides a complete and accurate display of this text.) ?

Shown Here:
Introduced in House (02/10/2020)

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "State and Local Cybersecurity Improvement Act".

SEC. 2. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

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

"SEC. 2215. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

"(a) ESTABLISHMENT.—The Secretary, acting through the Director, shall 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 (referred to as the 'State and Local Cybersecurity Grant Program' in this section).

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

"(1) The Cybersecurity Plan required under subsection (d) and approved pursuant to subsection (g).

"(2) The Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments required in accordance with section 2210, when issued.

"(c) ADMINISTRATION.—The State and Local Cybersecurity Grant Program shall be administered in the same program office that administers grants made under sections 2003 and 2004.

"(d) ELIGIBILITY.—

"(1) IN GENERAL.—A State applying for a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary a Cybersecurity Plan for approval. Such plan shall—

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

"(B) describe, to the extent practicable, how such State shall—

"(i) enhance the preparation, response, and resiliency of information systems owned or operated by such State or, if appropriate, by local, Tribal, or territorial governments, against cybersecurity risks and cybersecurity threats;

"(ii) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats in information systems of such State, local, Tribal, or territorial governments;

"(iii) ensure that State, local, Tribal, and territorial governments that own or operate information systems within the State adopt best practices and methodologies to enhance cybersecurity, such as the practices set forth in the cybersecurity framework developed by the National Institute of Standards and Technology;

"(iv) mitigate any identified gaps in the State, local, Tribal, or territorial government cybersecurity workforces, enhance recruitment and retention efforts for such workforces, and bolster the knowledge, skills, and abilities of State, local, Tribal, and territorial government personnel to address cybersecurity risks and cybersecurity threats;

"(v) ensure continuity of communications and data networks within such State between such State and local, Tribal, and territorial governments that own or operate information systems within such State in the event of an incident involving such communications or data networks within such State;

"(vi) assess and mitigate, to the greatest degree possible, cybersecurity risks and cybersecurity threats related to critical infrastructure and key resources, the degradation of which may impact the performance of information systems within such State;

"(vii) enhance capability to share cyber threat indicators and related information between such State and local, Tribal, and territorial governments that own or operate information systems within such State; and

"(viii) develop and coordinate strategies to address cybersecurity risks in consultation with—

"(I) local, Tribal, and territorial governments within the State; and

"(II) as applicable—

"(aa) neighboring States or, as appropriate, members of an information sharing and analysis organization; and

"(bb) neighboring countries; and

"(C) include, to the extent practicable, an inventory of the information technology deployed on the information systems owned or operated by such State or by local, Tribal, or territorial governments within such State, including legacy information technology that is no longer supported by the manufacturer.

"(e) PLANNING COMMITTEES.—

"(1) IN GENERAL.—A State applying for a grant under this section shall establish a cybersecurity planning committee to assist in the following:

"(A) The development, implementation, and revision of such State's Cybersecurity Plan required under subsection (d).

"(B) The determination of effective funding priorities for such grant in accordance with subsection (f).

"(2) COMPOSITION.—Cybersecurity planning committees described in paragraph (1) shall be comprised of representatives from counties, cities, towns, and Tribes within the State receiving a grant under this section, including, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

"(3) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMITTEES.—Nothing in this subsection may be construed to require that any State establish a cybersecurity planning committee if such State has established and uses a

multijurisdictional planning committee or commission that meets the requirements of this paragraph.

"(f) USE OF FUNDS.—A State that receives a grant under this section shall use the grant to implement such State's Cybersecurity Plan, or to assist with activities determined by the Secretary, in consultation with the Director, to be integral to address cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or territorial governments, as the case may be.

"(g) APPROVAL OF PLANS.—

"(1) APPROVAL AS CONDITION OF GRANT.—Before a State may receive a grant under this section, the Secretary, acting through the Director, shall review and approve such State's Cybersecurity Plan required under subsection (d).

"(2) PLAN REQUIREMENTS.—In approving a Cybersecurity Plan under this subsection, the Director shall ensure such Plan—

"(A) meets the requirements specified in subsection (d); and

"(B) upon issuance of the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments authorized pursuant to section 2210, complies, as appropriate, with the goals and objectives of such Strategy.

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

"(4) EXCEPTION.—Notwithstanding the requirement under subsection (d) to submit a Cybersecurity Plan as a condition of apply for a grant under this section, such a grant may be awarded to a State that has not so submitted a Cybersecurity Plan to the Secretary if—

"(A) such State certifies to the Secretary that it will submit to the Secretary a Cybersecurity Plan for approval by September 30, 2022;

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

"(C) such State certifies to the Secretary, and the Director confirms, that the activities that will be supported by the grant will address imminent cybersecurity risks or cybersecurity threats to the information systems of such State or of a local, Tribal, or territorial government in such State.

"(h) LIMITATIONS ON USES OF FUNDS.—

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

"(A) to supplant State, local, Tribal, or territorial funds;

"(B) for any recipient cost-sharing contribution;

"(C) to pay a demand for ransom in an attempt to regain access to information or an information system of such State or of a local, Tribal, or territorial government in such State;

"(D) for recreational or social purposes; or

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

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

"(i) OPPORTUNITY TO AMEND APPLICATIONS.—In considering applications for grants under this section, the Secretary shall provide applicants with a reasonable opportunity to correct defects, if any, in such applications before making final awards.

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

"(1) BASELINE AMOUNT.—The Secretary shall first apportion 0.25 percent of such amounts to each of American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, and the Virgin Islands, and 0.75 percent of such amounts to each of the remaining States.

"(2) REMAINDER.—The Secretary shall apportion the remainder of such amounts in the ratio that—

"(A) the population of each State; bears to

"(B) the population of all States.

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

"(1) For fiscal year 2021, 90 percent.

"(2) For fiscal year 2022, 80 percent.

"(3) For fiscal year 2023, 70 percent.

"(4) For fiscal year 2024, 60 percent.

"(5) For fiscal year 2025 and each subsequent fiscal year, 50 percent.

"(l) STATE RESPONSIBILITIES.—

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

"(2) AVAILABILITY OF FUNDS TO LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS.—Not later than 45 days after a State receives a grant under this section, such State shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local, Tribal, and territorial governments in such State, consistent with the applicable Cybersecurity Plan—

"(A) not less than 80 percent of funds available under such grant;

"(B) with the consent of such local, Tribal, and territorial governments, items, services, capabilities, or activities having a value of not less than 80 percent of the amount of the grant; or

"(C) with the consent of the local, Tribal, and territorial governments, grant funds combined with other items, services, capabilities, or activities having the total value of not less than 80 percent of the amount of the grant.

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

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

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

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

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

"(m) ADVISORY COMMITTEE.—

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

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

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

"(2) DUTIES.—The State and Local Cybersecurity Resiliency Committee shall—

"(A) submit to the Director recommendations that may inform guidance for applicants for grants under this section;

"(B) upon the request of the Director, provide to the Director technical assistance to inform the review of Cybersecurity Plans submitted by applicants for grants under this section, and, as appropriate, submit to the Director recommendations to improve

such Plans prior to the Director's determination regarding whether to approve such Plans;

"(C) advise and provide to the Director input regarding the Homeland Security Strategy to Improve Cybersecurity for State, Local, Tribal, and Territorial Governments required under section 2210; and

"(D) upon the request of the Director, provide to the Director recommendations, as appropriate, regarding how to—

"(i) address cybersecurity risks and cybersecurity threats on information systems of State, local, Tribal, or territorial governments;

"(ii) and improve the cybersecurity resilience of such governments.

"(3) MEMBERSHIP.—

"(A) NUMBER AND APPOINTMENT.—The State and Local Cybersecurity Resiliency Committee shall be composed of 15 members appointed by the Director, as follows:

"(i) Two individuals recommended to the Director by the National Governors Association.

"(ii) Two individuals recommended to the Director by the National Association of State Chief Information Officers.

"(iii) One individual recommended to the Director by the National Guard Bureau.

"(iv) Two individuals recommended to the Director by the National Association of Counties.

"(v) Two individuals recommended to the Director by the National League of Cities.

"(vi) One individual recommended to the Director by the United States Conference of Mayors.

"(vii) One individual recommended to the Director by the Multi-State Information Sharing and Analysis Center.

"(viii) Four individuals who have educational and professional experience related to cybersecurity analysis or policy.

"(B) TERMS.—Each member of the State and Local Cybersecurity Resiliency Committee shall be appointed for a term of two years, except that such term shall be three years only in the case of members who are appointed initially to the Committee upon the establishment of the Committee. Any member appointed to fill a vacancy occurring before the expiration of the term for which the member's predecessor was appointed shall be appointed only for the remainder of such term. A member may serve after the expiration of such member's term until a successor has taken office. A vacancy in the Commission shall be filled in the manner in which the original appointment was made.

"(C) PAY.—Members of the State and Local Cybersecurity Resiliency Committee shall serve without pay.

"(4) CHAIRPERSON; VICE CHAIRPERSON.—The members of the State and Local Cybersecurity Resiliency Committee shall select a chairperson and vice chairperson from among Committee members.

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

"(n) REPORTS.—

"(1) ANNUAL REPORTS BY STATE GRANT RECIPIENTS.—A State that receives a grant under this section shall annually submit to the Secretary a report on the progress of the State in implementing the Cybersecurity Plan approved pursuant to subsection (g). If the State does not have a Cybersecurity Plan approved pursuant to subsection (g), the State shall submit to the Secretary a report describing how grant funds were obligated and expended to develop a Cybersecurity Plan or improve the cybersecurity of information systems owned or operated by State, local, Tribal, or territorial governments in such State. The Secretary, acting through the Director, shall make each such report publicly available, including by making each such report available on the internet website of the Agency, subject to any redactions the Director determines necessary to protect classified or other sensitive information.

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

"(A) Achieving the objectives set forth in the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments, upon the strategy's issuance under section 2210.

"(B) Developing, implementing, or revising Cybersecurity Plans.

"(C) Reducing cybersecurity risks and cybersecurity threats to information systems owned or operated by State, local, Tribal, and territorial governments as a result of the award of such grants.

"(o) AUTHORIZATION OF APPROPRIATIONS.—There are authorized to be appropriated for grants under this section—

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

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

"(p) DEFINITIONS.—In this section:

"(1) CRITICAL INFRASTRUCTURE.—The term 'critical infrastructure' has the meaning given that term in section 2.

"(2) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given such term in section 102 of the Cybersecurity Act of 2015.

"(3) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in section 2209.

"(4) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency.

"(5) INCIDENT.—The term 'incident' has the meaning given such term in section 2209.

"(6) INFORMATION SHARING AND ANALYSIS ORGANIZATION.—The term 'information sharing and analysis organization' has the meaning given such term in section 2222.

"(7) INFORMATION SYSTEM.—The term 'information system' has the meaning given such term in section 102(9) of the Cybersecurity Act of 2015 (6 U.S.C. 1501(9)).

"(8) KEY RESOURCES.—The term 'key resources' has the meaning given that term in section 2.

"(9) STATE.—The term 'State'—

"(A) means each of the several States, the District of Colombia, and the territories and possessions of the United States; and

"(B) includes any federally recognized Indian tribe that notifies the Secretary, not later than 120 days after the date of the enactment of this section or not later than 120 days before the start of any fiscal year in which a grant under this section is awarded, that the tribe intends to develop a Cybersecurity Plan and agrees to forfeit any distribution under subsection (l)(2).".

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

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

SEC. 3. STRATEGY.

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

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

"(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this subsection, the Secretary, acting through the Director, shall, in coordination with appropriate Federal departments and agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee (established under section 2215), and other stakeholders, as appropriate, develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments that provides recommendations regarding how the Federal Government should support and promote the ability State, local, Tribal, and territorial

governments to identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents (as such term is defined in section 2209) and establishes baseline requirements and principles to which Cybersecurity Plans under such section shall be aligned.

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

"(A) identify capability gaps in the ability of State, local, Tribal, and territorial governments to identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents;

"(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to help such governments identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents;

"(C) identify and assess the limitations of Federal resources and capabilities available to State, local, Tribal, and territorial governments to help such governments identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents, and make recommendations to address such limitations;

"(D) identify opportunities to improve the Agency's coordination with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve incident exercises, information sharing and incident notification procedures, the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives, and opportunities to leverage Federal schedules for cybersecurity investments under section 502 of title 40, United States Code;

"(E) recommend new initiatives the Federal Government should undertake to improve the ability of State, local, Tribal, and territorial governments to help such governments identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents;

"(F) set short-term and long-term goals that will improve the ability of State, local, Tribal, and territorial governments to help such governments identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents; and

"(G) set dates, including interim benchmarks, as appropriate for State, local, Tribal, territorial governments to establish baseline capabilities to identify, prepare for, detect, protect against, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents.

"(3) CONSIDERATIONS.—In developing the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments required under paragraph (1), the Director, in coordination with appropriate Federal departments and agencies, State, local, Tribal, and territorial governments, the State and Local

Cybersecurity Resilience Committee, and other stakeholders, as appropriate, shall consider—

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

"(B) the impact of incidents that have affected State, local, Tribal, and territorial governments, including the resulting costs to such governments;

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

"(D) emerging cybersecurity risks to State, local, Tribal, and territorial governments resulting from the deployment of new technologies; and

"(E) recommendations made by the State and Local Cybersecurity Resilience Committee.".

(b) RESPONSIBILITIES OF THE DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.—Subsection (c) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended—

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

(2) by inserting after paragraph (5) the following new paragraphs:

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

"(7) review, in consultation with the State and Local Cybersecurity Resiliency Committee, all cybersecurity plans of State, local, Tribal, and territorial governments developed pursuant to any homeland security assistance administered by the Department to improve cybersecurity;

"(8) provide expertise and technical assistance to State, local, Tribal, and territorial government officials with respect to cybersecurity;

"(9) provide education, training, and capacity development to enhance the security and resilience of cybersecurity and infrastructure security;".

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