The Cybersecurity and Infrastructure Security Agency's protective security advisers help improve security at schools, places of worship, and other soft targets, but there are too few of them to meet the demand of their services.

H.R. 5780 would require CISA to maintain an online security resources clearinghouse to provide security guidance and best practices, serving as a one-stop shop for school districts, religious organizations, and local officials to find the information they need to keep their communities safe.

The bill would also require CISA to develop a stakeholder outreach and operational engagement strategy and implementation plan to ensure that the Agency is delivering infrastructure security services across sectors and throughout regions.

Finally, H.R. 5780 would authorize a PSA force multiplier pilot program, which would require CISA PSAs to train State, local, Tribal, and territorial officials to perform security vulnerability and terrorism risk assessments. These risk assessments are an important part of qualifying for FEMA's security grants; the force multiplier program will help expand access to them.

I am proud that the Safe Communities Act of 2020 has been endorsed by the Jewish Federations of North America and the Anti-Defamation League.

I would like to thank my colleague, Mr. KATKO, for joining me in introducing this measure. I am grateful for his collaboration and leadership as ranking member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation.

I want to extend my sincere appreciation to the Homeland Security Committee staff for their work on this legislation.

I urge my colleagues on both sides of the aisle to support this legislation today to make sure every community in America has the resources it needs to keep people safe.

I urge my colleagues to support H.R. 5780, and I reserve the balance of my time.

Mr. JOYCE of Pennsylvania. Mr. Speaker, I yield myself such time as I may consume.

I rise in support of H.R. 5780. This bill makes the great work done by the Cybersecurity and Infrastructure Security Agency more accessible to stakeholders.

CISA provides advice and recommendations upon the request of critical infrastructure owners and operators on how to secure and protect their facilities in cyberspace and physically.

This bill will help stakeholders clearly know what CISA can do. Continuing to develop the relationship between CISA and our private stakeholders remains an integral piece of our critical infrastructure security.

I thank Representatives UNDERWOOD and KATKO for their bill.

Mr. Speaker, I urge a ''yes'' vote on the bill, and I yield back the balance of my time.

Ms. UNDERWOOD. Mr. Speaker, I yield myself such time as I may consume.

Last week, I was appointed as the new chair of the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation of the Homeland Security Committee. It is a great honor and opportunity for me to amplify the homeland security concerns of the people of Illinois' 14th Congressional District here in Washington.

□ 1330

My constituents are concerned about the vulnerability of so-called soft targets to violence. CISA, which is overseen by my subcommittee, has a critical role to play to empower communities to be more secure and resilient against ever-increasing lists of homeland security threats.

I am committed to ensuring the success of the PSA program, and I look forward to working with CISA to make sure that every community can benefit from it. Enactment of the Safe Communities Act of 2020 will help CISA think more strategically about how it deploys PSAs and other services and do so in a way that will scale.

Mr. Speaker, I urge my colleagues to support the measure, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Illinois (Ms. UNDERWOOD) that the House suspend the rules and pass the bill, H.R. 5780, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

STATE AND LOCAL CYBERSECURITY IMPROVEMENT ACT

Ms. UNDERWOOD. Mr. Speaker, I move to suspend the rules and pass the bill (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, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5823

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 sections:

''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) promote the delivery of safe, recognizable, and trustworthy online services by State, local, Tribal, and territorial governments, including through the use of the .gov internet domain;

''(v) 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;

''(vi) 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;

''(vii) 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;

''(viii) 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

''(ix) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats 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) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency.

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

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

''(6) 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)).

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

''(8) ONLINE SERVICE.—The term 'online service' means any internet-facing service, including a website, email, virtual private network, or custom application.

''(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).

''SEC. 2216. CYBERSECURITY RESOURCE GUIDE DEVELOPMENT FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT OFFICIALS.

''The Secretary, acting through the Director, shall develop a resource guide for use by State, local, Tribal, and territorial government officials, including law enforcement officers, to help such officials 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).''.

(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 items:

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

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

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, protect against, detect 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, protect against, detect, 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, protect against, detect, 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, protect against, detect, 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, protect against, detect, 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, protect against, detect, 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, protect against,

detect, 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 and cybersecurity threats 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 (11) through (16), 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;

''(10) provide information to State, local, Tribal, and territorial governments on the security benefits of .gov domain name registration services;''.

(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.

The SPEAKER pro tempore. Pursuant to the rule, the gentlewoman from Illinois (Ms. UNDERWOOD) and the gentleman from Pennsylvania (Mr. JOYCE) each will control 20 minutes.

The Chair recognizes the gentlewoman from Illinois.

GENERAL LEAVE

Ms. UNDERWOOD. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days to revise and extend their remarks and to include extraneous material on this measure.

The SPEAKER pro tempore. Is there objection to the request of the gentlewoman from Illinois?

There was no objection.

Ms. UNDERWOOD. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I don't need to tell anyone here that cyberattacks against State and local governments are growing more frequent and more sophisticated. In 2019, there were over 100 ransomware attacks on State and local governments.

From major cities like New Orleans and Baltimore to small towns across Texas, cyberattacks sought to cripple the ability of governments across the country to carry out basic functions, from processing real estate transactions to collecting payments for services.

The cost is more than just a mere inconvenience. A ransomware attack against a State and local government can disrupt lifeline services, like 911 call centers and public hospitals, and extort money those governments do not have.

Last summer, the mayor of Atlanta, Keisha Lance Bottoms, testified before my subcommittee that the ransomware attack that hit her city in 2018 cost city taxpayers $7.2 million to recover from, but experts expect that cost to grow to as much as $17 million.

The COVID–19 pandemic, by dramatically expanding the threat landscape and making government networks more attractive targets for hackers, has made the situation more dire. More Americans than ever before are working from home. That includes State and local government workers who may be less accustomed to teleworking and less prepared to do it securely.

At the same time, the cyber risk to State and local networks has increased dramatically due to unprecedented demand for online services, including unemployment compensation and human services applications.

The transition to online learning that COVID–19 has forced many schools to undertake has also not been without incident. According to Education Week, there have been 220 cyberattacks against schools so far this year. And while the pandemic is bringing the vulnerability of our school districts' networks into focus, it is worth noting that there have been over 1,000 cyberattacks against school districts since 2016, according to the K–12 Research Center.

Despite the urgent need to address their cyber vulnerabilities, many State and local governments are not in a position to do so without outside assistance, as they are overwhelmed by the challenges of maintaining basic services in the face of steep COVID–19-related revenue losses.

It is time for the Federal Government to step up and help. Passing H.R. 5823, the State and Local Cybersecurity Improvement Act, which I am proud to cosponsor, is an important first step.

The bill would establish a $400 million targeted grant program to help States and local governments develop robust cybersecurity capabilities. Importantly, it requires States to pay a graduated match to incentivize them to budget better for cybersecurity.

And it requires the Department of Homeland Security to create a plan to improve the cybersecurity posture of State and local governments to ensure that Federal resources align with State goals and objectives. The smart investments we make in the cybersecurity of our State and local governments now will pay for themselves in the future.

Mr. Speaker, I urge my colleagues to support H.R. 5823, and I reserve the balance of my time.

Mr. JOYCE of Pennsylvania. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise in strong support of H.R. 5823.

Preparing our State, local, Tribal, and territorial governments for the increasing number of cyber threats they face is a necessary priority.

Cybersecurity preparedness is ineffective if our only focus is on Federal preparedness. It is incumbent on us to ensure that our State and local partners are taking advantage of the resources that we can offer so they, too, can prepare for the threats that they might face. H.R. 5823 will do just that. It establishes a matching grant program for State and local governments to access and close vulnerabilities in their IT systems.

Mr. Speaker, I thank Representatives Richmond and Katko for their bill, and I reserve the balance of my time.

Ms. UNDERWOOD. Mr. Speaker, I yield 2 minutes to the gentleman from Maryland (Mr. RUPPERSBERGER).

Mr. RUPPERSBERGER. Mr. Speaker, I thank the gentlewoman for yielding.

Before I start, I want to acknowledge the gentlewoman's leadership position. I was sitting in my chair—I have been dealing with cyber issues for a long time—and when I heard Mr. JOYCE agree with the gentlewoman, I almost fell out of my chair, but I didn't. I really applaud both Members for working together.

Cyber issues are some of the most important national security issues that our country faces, internationally and also within our country, and coming together like this is how we get things done for our constituents. I hope people on both sides of the aisle observe what these Representatives are doing. That is the way we need to go.

First, as a former Baltimore County executive, I am well aware of the problems that State and local governments face on a daily basis. They are where

the rubber meets the road and the source of many of the critical services our constituents rely on, which includes schools, law enforcement, parks, fire, and libraries.

Yet, according to the National Association of State Chief Information Officers, nearly half of all States do not have a dedicated cybersecurity line item in their budget. In fact, most State cybersecurity budgets are between 0 and 3 percent of their overall information technology budget.

While some support from the Federal Government does exist already, less than 4 percent of current Homeland Security Grant Program funding has been allocated to cybersecurity needs at the State and local level. As we have seen from recent cyberattacks on many American cities and States, this is simply not enough.

Last year, there were at least 24 public-sector ransomware attacks, including a ransomware attack in Baltimore, my hometown, that is expected to cost more than $18 million in remediation. A separate attack in 2018 temporarily disabled Baltimore's 911 dispatch system.

This is part of a growing nationwide trend. The COVID–19 pandemic has only exacerbated the threat to local governments as hackers exploit overwhelmed organizations that are increasingly dependent on digital tools. We cannot simply stand by and watch this happen. We can and must do more.

The SPEAKER pro tempore. The time of the gentleman has expired.

Ms. UNDERWOOD. Mr. Speaker, I yield the gentleman from Maryland an additional 2 minutes.

Mr. RUPPERSBERGER. Mr. Speaker, the bill before us today establishes a program making grants available to State, local, Tribal, and territorial governments to address cybersecurity risks and threats to their information systems.

This is not a silver bullet, but it allows us to leverage Federal expertise in cyber, like that of the Cybersecurity and Infrastructure Security Agency, or CISA, to help State and local governments get their information security programs off the ground.

This bill will further empower State and local governments around the country to begin assuming the funding burden in their normal budget cycles in the future by reducing the Federal share over time.

I thank Chairman THOMPSON, Chairman RICHMOND, and all those involved for this bipartisan coalition.

Ms. UNDERWOOD. Mr. Speaker, I yield 3 minutes to the gentleman from Washington (Mr. KILMER).

Mr. KILMER. Mr. Speaker, I thank my good friend for yielding and echo the gratitude for her leadership and the bipartisan leadership of the subcommittee.

Mr. Speaker, I rise in strong support of the State and Local Cybersecurity Improvement Act, a bipartisan bill that I was proud to help introduce, to deliver urgently needed investments to address the vulnerabilities that persist in State, local, Tribal, and territorial cyber infrastructures.

These cyber threats are real, and our communities need help.

I have spoken with a county auditor just recently who said she is conscious that her systems are constantly targeted.

I have spoken with public power providers who understand that, in the absence of sufficient cybersecurity, we could see an attack that would wipe out our critical utilities for citizens and could undermine our economy.

I have recently spoken with a Tribal leader who said that they have enough technology challenges without seeing the threat of cyberattack compound things.

I have spoken with a county hospital in my district that was hit by a ransomware attack.

This bill is about letting those folks know and the people whom they serve know that they are not on their own, that the Federal Government understands that cybersecurity vulnerabilities don't only exist in marble buildings in Washington, D.C., but that they exist in communities in every State in our Nation, and with this bill the Federal Government says: We are going to have your back. That is why I urge my colleagues on both sides of the aisle to support this bipartisan plan. There is no time to waste.

Ms. UNDERWOOD. Mr. Speaker, I have no more speakers, and I am prepared to close after the gentleman from Pennsylvania closes. I reserve the balance of my time.

Mr. JOYCE of Pennsylvania. Mr. Speaker, I urge a ''yes'' vote on the bill, and I yield back the balance of my time.

Ms. UNDERWOOD. Mr. Speaker, over the past decade and a half, Congress has redoubled efforts to secure Federal networks. This legislation will continue that work by supporting State and local cybersecurity improvements. It was approved on a bipartisan basis in committee and has broad and deep support within stakeholder communities.

I would like to congratulate Congressman CEDRIC RICHMOND, the former chairman of the Cybersecurity, Infrastructure Protection, and Innovation Subcommittee, on this important legislation.

Mr. Speaker, I urge my colleagues to support the measure, and I yield back the balance of my time.

The SPEAKER pro tempore. The question is on the motion offered by the gentlewoman from Illinois (Ms. UNDERWOOD) that the House suspend the rules and pass the bill, H.R. 5823, as amended.

The question was taken; and (two-thirds being in the affirmative) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

□ 1345

HOMELAND SECURITY ACQUISITION PROFESSIONAL CAREER PROGRAM ACT

Ms. UNDERWOOD. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 5822) to amend the Homeland Security Act of 2002 to establish an acquisition professional career program, and for other purposes, as amended.

The Clerk read the title of the bill.

The text of the bill is as follows:

H.R. 5822

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 ''Homeland Security Acquisition Professional Career Program Act''.

SEC. 2. AUTHORIZATION OF THE ACQUISITION PROFESSIONAL CAREER PROGRAM.

(a) IN GENERAL.—Title VII of the Homeland Security Act of 2002 (6 U.S.C. 341 et seq.) is amended by adding at the end the following new section:

''SEC. 711. ACQUISITION PROFESSIONAL CAREER PROGRAM.

''(a) ESTABLISHMENT.—There is established in the Department an acquisition professional career program to develop a cadre of acquisition professionals within the Department.

''(b) ADMINISTRATION.—The Under Secretary for Management shall administer the acquisition professional career program established pursuant to subsection (a).

''(c) PROGRAM REQUIREMENTS.—The Under Secretary for Management shall carry out the following with respect to the acquisition professional career program.

''(1) Designate the occupational series, grades, and number of acquisition positions throughout the Department to be included in the program and manage centrally such positions.

''(2) Establish and publish on the Department's website eligibility criteria for candidates to participate in the program.

''(3) Carry out recruitment efforts to attract candidates—

''(A) from institutions of higher education, including such institutions with established acquisition specialties and courses of study, historically Black colleges and universities, and Hispanic-serving institutions;

''(B) with diverse work experience outside of the Federal Government; or

''(C) with military service.

''(4) Hire eligible candidates for designated positions under the program.

''(5) Develop a structured program comprised of acquisition training, on-the-job experience, Department-wide rotations, mentorship, shadowing, and other career development opportunities for program participants.

''(6) Provide, beyond required training established for program participants, additional specialized acquisition training, including small business contracting and innovative acquisition techniques training.

''(d) REPORTS.—Not later than December 31, 2020, and annually thereafter through 2026, the Secretary shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report on the acquisition professional career program. Each such report shall include the following information:

''(1) The number of candidates approved for the program.