116TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
116–478

STATE AND LOCAL CYBERSECURITY IMPROVEMENT ACT

AUGUST 18, 2020.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. THOMPSON of Mississippi, from the Committee on Homeland Security, submitted the following

R E P O R T

[To accompany H.R. 5823]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security, to whom was referred 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, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

	Page
Purpose and Summary	8
Background and Need for Legislation	9
Hearings	10
Committee Consideration	11
Committee Votes	12
Committee Oversight Findings	12
C.B.O. Estimate, New Budget Authority, Entitlement Authority, and Tax Expenditures	13
Federal Mandates Statement	14
Duplicative Federal Programs	14
Statement of General Performance Goals and Objectives	14
Congressional Earmarks, Limited Tax Benefits, and Limited Tariff Benefits	15
Advisory Committee Statement	
Applicability to Legislative Branch	
Section-by-Section Analysis of the Legislation	15
Changes in Existing Law Made by the Bill, as Reported	18

The amendment is as follows:

Strike all after the enacting clause and insert the following:

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 stake-

holder 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; and

"(ii) 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 Cybersecu-

rity 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 nonstate 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.

PURPOSE AND SUMMARY

H.R. 5823, the "State and Local Cybersecurity Improvement Act" seeks to foster a stronger partnership between the Federal government and State and local governments to defend their State and local networks against the cyberattacks from sophisticated foreign adversaries or cyber criminals. One critical provision would authorize a new Department of Homeland Security (DHS) grant program to address cybersecurity vulnerabilities on State and local government networks. The new grant program would be authorized at $400 million with a graduating cost-share that incentivizes States to increase funding for cybersecurity in their budgets. Under the bill, State, tribal, and territorial governments would be required to develop comprehensive cybersecurity plans to guide the use of grant funds. The bill also requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop a strategy to improve the cybersecurity of State, local, Tribal, and territorial governments, set baseline objectives for State and local cybersecurity efforts, and, among other things, identify Federal resources that could be made available to State and local governments for cybersecurity purposes. CISA would also be required 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 at CISA. Lastly, the bill establishes a State and Local Cybersecurity Resiliency Committee comprised of representatives from State, local, Tribal, and territorial governments to advise and provide situational awareness to CISA regarding the cybersecurity needs of such governments.

BACKGROUND AND NEED FOR LEGISLATION

Like Federal agencies, State and local governments are rich targets for cyber adversaries given the volume of sensitive personal data they house and the high cost that a service disruption and system failures would impose. However, State and local agencies tend to have far fewer resources and cybersecurity personnel than their counterparts at the Federal level, or compared to similarly-sized private sector entities.[1]

At the State level, cybersecurity responsibilities are generally carried out by a Chief Information Security Officer (CISO). Until recently, CISOs did not exist in many states or remained vacant.[2] Today, every state has an enterprise-level CISO recognized in State law or other administrative procedures.[3] Although role of the state CISO has matured dramatically, turnover among state CISOs remains high. Moreover, CISOs consistently report budgetary and personnel shortages as among their top concerns.[4]

Cybersecurity challenges are particularly acute at the local level, where resources are often scarce. A 2016 survey by the International City/County Management Association (ICMA) found that nearly 40% of local government Chief Information Officers (CIOs) reported having experienced an attack during the last 12 months, and 26% reported an attack, incident, or breach attempt occurring hourly.[5] At the same time, many local governments are not well prepared to recover from a ransomware attack, detect or prevent exfiltration, prefect and recover from breaches, or detect attacks.[6] Moreover, many local officials and staff are not sufficiently aware of the need for cybersecurity.[7]

In 2018, devastating ransomware attacks crippled Atlanta, Georgia. The following year, State and local agencies in Louisiana, the City of Baltimore, MD, 22 towns in Texas, a school district in Syracuse, NY and many other communities scattered across the country were impacted by disruptive ransomware attacks. One DHS official described the ransomware attack in Atlanta as "one of those red blinking lights that people talk about—it's a warning bell," and observed that "the attack surface is expanding faster . . . than we are fixing the legacy IT landscape."[8] These attacks can be extremely disruptive to vital government services and recovery is often far costlier than anticipated—to the tune of nearly $20 million, in some cases.[9]

---

[1] National Association of State Chief Information Security Officers (NASCIO), *2018 Deloitte-NASCIO Cybersecurity Study: States at Risk* (Oct. 2018), https://www.nascio.org/Publications/ArtMID/485/ArticleID/730/2018-Deloitte-NASCIO Cybersecurity-Study-States-at-risk-Bold-plays-for-change.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] International City/County Management Association and University of Maryland Baltimore County, *Cybersecurity 2016 Survey,* https://icma.org/sites/default/files/309075_2016%20cybersecurity%20survey_summary%20report_final.pdf.

[6] Donald Norris, et. al, "Local Governments" Cybersecurity Crisis in 8 Charts," *Government Technology* (April 30, 2018), https://www.govtech.com/security/Local-Governments-Cybersecurity-Crisis-in-8-Charts.html.

[7] *Id.*

[8] "Atlanta Ransomware Attack a 'Warning Bell,' DHS Official Says," *Meritalk* (April 28, 2018), https://www.meritalk.com/articles/atlanta-ransomware-attack-a-warning-bell-dhs-official-says/.

[9] *See* Ian Duncan, "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million As Government Begins To Restore Email Accounts," *The Baltimore Sun* (May 29, 2019), https://

Continued

Stretched State and local budgets have not adequately funded cybersecurity and, with the emergence of the COVID–19 pandemic in 2020, existing cybersecurity challenges at the State and local level have been exacerbated. The global COVID–19 pandemic changed every aspect of American life. According the Brookings Institution, by April 2020, "up to half of American workers are currently working from home." [10] That includes State and local government employees who may be less accustomed to teleworking and less prepared to do it securely, making State and local networks more vulnerable to ransomware and other cyber attacks. At the same time, the cyber risks to State and local networks increased dramatically, particularly in the wake of unprecedented demand for online services, such as unemployment compensation and human services applications.[11]

To address this urgent national security issue, the Federal government needs to redouble its efforts at partnering with State and local governments to build robust cybersecurity defenses. The "State and Local Cybersecurity Improvement Act" requires both the Federal government and its State partners to develop strategies to bolster State and local cybersecurity capabilities and provides funding to ensure those strategies are implemented. Investing in cybersecurity before a cyberattack saves money, protects important data housed on State and local networks, and ensures State and local governments can continue to provide the important services Americans rely on.

H.R. 5823 has been endorsed by the National Governors Association and National Association of State Chief Information Security Officers.

HEARINGS

For the purposes of section 103(i) of H. Res 6. of the 116th Congress, the following hearing was used to develop H.R. 5823:

- On Tuesday, June 25, 2019, the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled: "Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help." The following witnesses testified: Hon. Keisha Lance Bottoms, Mayor of Atlanta, Georgia; Mr. Thomas Duffy, Senior Vice President of Operations, Center for Internet Security, and Chair of the Multi-State Information Sharing and Analysis Center (MS–ISAC); Mr. Ahmad Sultan, Associate Director, Anti-Defamation League Center for Technology and Society, and former Fellow at the Center for Long Term Cybersecurity, University of California Berkeley; Mr. Frank J. Cilluffo, Direc-

---

www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.

[10] Katherine Guyot & Isabel V. Sawhill, "Telecommuting Will Likely Continue Long After the Pandemic," blog, Brookings Institution (Apr. 6, 2020), https://www.brookings.edu/blog/up-front/2020/04/06/telecommuting-will-likely-continue-long-after-the-pandemic/.

[11] Letter to Majority Leader Mitch McConnell, Speaker Nancy Pelosi, Senate Democratic Leader Chuck Schumer, and House Republican Leader Kevin McCarthy from National Governors Association; Government Finance Officers Association; Governors Homeland Security Advisors Council; International City/County Management Association; National Association of Counties; National Association of State Auditors, Comptrollers and Treasurers; National Association of State Chief Information Officers; National Association of State Treasurers; National Conference of State Legislatures; National Emergency Management Association; National League of Cities; and The Council of State Governments (Apr. 28, 2020).

tor, McCrary Institute for Cyber and Critical Infrastructure, Auburn University.

COMMITTEE CONSIDERATION

The Committee met on February 12, 2020, with a quorum being present, to consider H.R. 5823 and ordered the measure to be reported to the House with a favorable recommendation, with amendments, by unanimous consent.

The following amendments were offered:

An amendment offered by Mr. Katko.

Page 2, line 5, strike "section" and insert "sections".

Page 21, line 4, strike the closing quotes and the second period.

Page 21, after line 4, insert the following:

"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).".

Page 21, beginning line 5, strike subsection (b) and insert the following:

(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.".

An amendment offered by Mr. Langevin.

Page 4, beginning line 11, insert the following:

"(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;".

Page 20, beginning line 17, insert the following:

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

Page 26, beginning line 5, strike "paragraphs (6) through (11) as paragraphs (10) through (15)" and insert "paragraphs (6) through (11) as paragraphs (11) through (16)".

Page 27, line 3, strike the closing quotes and the second period.

Page 27, beginning line 4, insert the following:

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

An amendment offered by Mr. Richmond.

Page 5, line 17, insert "and cybersecurity threats" after "cybersecurity risks".

Page 19, strike lines 21 through 23.

Page 22, line 7, strike "prepare for, detect, protect against" and insert "protect against, detect".

Page 22, line 19, strike "prepare for, detect, protect against" and insert "protect against, detect".

Page 23, line 2, strike "prepare for, detect, protect against" and insert "protect against, detect".

Page 23, beginning line 8, strike "prepare for, detect, protect against" and insert "protect against, detect".

Page 24, line 5, strike "prepare for, detect, protect against" and insert "protect against, detect".

Page 24, beginning line 11, strike "prepare for, detect, protect against" and insert "protect against, detect".

Page 24, beginning line 18, strike "prepare for, detect, protect against" and insert "protect against, detect".

Page 25, line 19, insert "and cybersecurity threats" after "cybersecurity risks".

An amendment offered by Ms. Slotkin.

Page 6, beginning line 10, insert the following:

(2) DISCRETIONARY ELEMENTS.—The Cybersecurity Plan of a State described in paragraph (1) may include—

(A) cooperative programs developed by groups of local, Tribal, and territorial governments within such State to address cybersecurity risks and cybersecurity threats; and

(B) programs provided by such State to support local, Tribal, and territorial governments and critical infrastructure owners and operators to address cybersecurity risks and cybersecurity threats.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the recorded votes on the motion to report legislation and amendments thereto.

No recorded votes were requested during consideration of H.R. 5823.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

CONGRESSIONAL BUDGET OFFICE ESTIMATE, NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

With respect to the requirements of clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the Congressional Budget Act of 1974 and with respect to requirements of clause (3)(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the Congressional Budget Act of 1974, the Committee adopts as its own the estimate of the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office.

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, March 10, 2020.

Hon. BENNIE G. THOMPSON,
Chairman, Committee on Homeland Security,
House of Representatives, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 5823, the State and Local Cybersecurity Improvement Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prosperi.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

H.R. 5823, State and Local Cybersecurity Improvement Act
As ordered reported by the House Committee on Homeland Security on February 12, 2020

By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	872	not estimated

Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2031?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

* = between zero and $500,000.

H.R. 5823 would authorize the appropriation of $400 million annually over the 2021–2025 period for the Department of Homeland Security (DHS) to award grants to state and local governments. Grant recipients would use those funds to address cybersecurity threats and risks to their information systems. The bill also would establish the process through which DHS would assess grant applications, review cybersecurity plans, and monitor the performance of grant recipients.

Based on historical spending patterns for similar grant programs, CBO estimates that implementing H.R. 5823 would cost $872 million over the 2020–2025 period (detailed in Table 1). Such spending would be subject to the appropriationof the specified and estimated amounts. That estimate includes $15 million in salaries and expenses over the 2020–2025 period for administrative costs of reviewing grant applications and cybersecurity plans, and communicating with state and local governments. It also includes $5 million for the costs of establishing an external advisory committee.

For this estimate, CBO assumes that the bill will be enacted in fiscal year 2020. Under that assumption, the agency could incur some costs in 2020, but CBO expects that most of the costs would be incurred in 2021 and later.

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER H.R. 5823

	By fiscal year, millions of dollars—						
	2020	2021	2022	2023	2024	2025	2020–2025
Cybersecurity Grants:							
Authorization	0	400	400	400	400	400	2,000
Estimated Outlays	0	12	84	164	256	336	852
Administrative Costs:							
Estimated Authorization	*	2	2	3	4	4	15
Estimated Outlays	*	2	2	3	4	4	15
Advisory Committee:							
Estimated Authorization	*	1	1	1	1	1	5
Estimated Outlays	*	1	1	1	1	1	5
Total Changes:							
Estimated Authorization	*	403	403	404	405	405	2,020
Estimated Outlays	*	15	87	168	261	341	872

* = between zero and $500,000.

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 5823 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the objective of H.R. 5823 is to direct the Department of Homeland Security to help State and local governments improve the cybersecurity posture of State, local, Tribal, and territorial governments. To achieve this objective, the Department will be required to engage with appropriate stakeholders to develop a comprehensive Homeland Security Strategy to Improve the Cy-

bersecurity of State, Local, Tribal, and Territorial Governments to which grantees can align their cybersecurity plans.

ADVISORY ON EARMARKS

In compliance with rule XXI of the Rules of the House of Representatives, this bill, as reported, contains no congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(f) of the rule XXI.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This section provides that this bill may be cited as the "State and Local Cybersecurity Grant Program."

Sec. 2. State and Local Cybersecurity Grant Program

This section directs the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Security Agency, 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 that is administered by the Federal Emergency Management Agency. The program will be referred to as the State and Local Cybersecurity Grant Program.

This section further requires each State seeking funds under the State and Local Cybersecurity Grant Program to develop and submit to the Secretary for approval a cybersecurity plan and establishes the baseline requirements for cybersecurity plans.

This section further requires each State seeking funds under the State and Local Cybersecurity Grant Program to establish a cybersecurity planning committee to assist in the development and implementation of cybersecurity plans and in prioritizing State and Local Cybersecurity Grant Program investments. The cybersecurity planning committees shall be comprised of representatives from counties, cities, towns, and Tribes within the State receiving a grant, including, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

This section further describes permissible uses of grants awarded under the State and Local Cybersecurity Grant Program to include implementing a State's cybersecurity plan, or assisting with activities determined by the Secretary, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, 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.

This section requires the Secretary, acting through the Director of the Cybersecurity and Infrastructure Agency, to review State cybersecurity plans to ensure they comport with the baseline requirements set forth in the section and the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments. State cybersecurity plans must be approved by the Secretary before a State may receive grant funds, unless the State certifies that it will submit a cybersecurity plan by September 30, 2020, and grant funds will be used to develop the cybersecurity

plan or the grant will address imminent cybersecurity risks or cybersecurity threats.

This section bars the use of State and Local Cybersecurity Grant Program funds to supplant State, local, Tribal, or territorial funds; for any recipient cost-sharing contribution; 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; for recreational or social purposes; or 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. States must certify that it will use grant funds for an appropriate purpose. The Secretary is authorized to take such enforcement actions necessary.

This section also authorizes States to amend grant applications to correct defects, sets forth the formula the Secretary shall use to apportion grant awards to eligible grantees, and establishes a State cost-share that increases over time to incentivize States to invest in cybersecurity.

This section requires States (but not territories) to make 80 percent grant funds available to local and Tribal governments within 45 days of receiving the grant award, with certain exceptions. States are required to certify compliance with distribution requirements to the Secretary. If a State fails to make funds available to local and Tribal governments in compliance with this Act, local and Tribal governments may seek direct funding from the Secretary. The Secretary may impose appropriate penalties to enforce this provision.

This section directs the Director of the Cybersecurity and Infrastructure Security Agency to establish a State and Local Cybersecurity Resilience Committee to advise the Director on matters relating to cybersecurity matters particular to State and Local governments, help review State cybersecurity plans, provide feedback on the Homeland Security Strategy to Improve Cybersecurity for State, Local, Tribal, an Territorial Governments, and to assist in the development of State and Local Cybersecurity Grant guidance. This section also describes the membership and terms of the State and Local Cybersecurity Resilience Committee, and provides that the members shall not receive compensation.

This section requires States receiving a grant to annually submit a report on the progress of the State in implementing the approved cybersecurity plan to the Secretary. If the State does not have an approved cybersecurity plan, 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. The Committee expects the Secretary to establish consist framework for the annual report, including consistent metrics and categories of analysis, so Congress is able assess how grant funds are supporting the improvement in the cybersecurity posture of State, local, Tribal, and territorial governments. The Committee

further expects the report to include information on the use, or barriers to use, of .gov domain services by State, local, Tribal, and territorial governments.

This section requires the Secretary to submit a report to Congress annually on the use of grant funds and progress achieving the objectives set forth in the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments, among other things.

This section authorizes $400,000,000 in appropriations for this grant program from FY 2021 through FY 2025, and such sums necessary thereafter.

Sec. 3. Strategy

This section requires the Secretary, acting through the Director of the Cybersecurity and Infrastructure Security Agency, to 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.

This section requires that, not later than 270 days after the date of the enactment, the Secretary, acting through the Director, to develop and make publicly available, 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, 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 of State, local, Tribal, and territorial governments to identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, and incidents and establishes baseline requirements and principles to which State cybersecurity plans under such section shall be aligned. The Committee expects the Department of Homeland Security to submit budget or legislative proposals, as necessary, to address any resource or authority gaps identified.

This section further describes the contents of the Homeland Security Strategy to Improve the Cybersecurity of State, Local Tribal, and Territorial Governments, as well as considerations that should inform the strategy. The Committee expects the Cybersecurity and Infrastructure Security Agency to emphasize to State, local, Tribal, and territorial governments the benefits of .gov domain services.

This section amends the responsibilities of the Director of the Cybersecurity and Infrastructure Security Agency related to the Director's responsibilities related to improving the cybersecurity of State and local governments.

This section requires the Director of the Cybersecurity and Infrastructure Security Agency to, not later than 180 days after the date of the enactment of this Act, 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.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italics, and existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Homeland Security Act of 2002".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

Sec. 2215. State and Local Cybersecurity Grant Program.
Sec. 2216. Cybersecurity resource guide development for State, local, Tribal, and territorial government officials.

* * * * * * *

TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Subtitle A—Cybersecurity and Infrastructure Security

* * * * * * *

SEC. 2202. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) REDESIGNATION.—

(1) IN GENERAL.—The National Protection and Programs Directorate of the Department shall, on and after the date of the enactment of this subtitle, be known as the "Cybersecurity and Infrastructure Security Agency" (in this subtitle referred to as the "Agency").

(2) REFERENCES.—Any reference to the National Protection and Programs Directorate of the Department in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Cybersecurity and Infrastructure Security Agency of the Department.

(b) DIRECTOR.—

(1) IN GENERAL.—The Agency shall be headed by a Director of Cybersecurity and Infrastructure Security (in this subtitle referred to as the "Director"), who shall report to the Secretary.

(2) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cy-

bersecurity, and any other related program of the Department as described in section 103(a)(1)(H) as in effect on the day before the date of enactment of this subtitle in any law, regulation, map, document, record, or other paper of the United States shall be deemed to be a reference to the Director of Cybersecurity and Infrastructure Security of the Department.

(c) RESPONSIBILITIES.—The Director shall—

(1) lead cybersecurity and critical infrastructure security programs, operations, and associated policy for the Agency, including national cybersecurity asset response activities;

(2) coordinate with Federal entities, including Sector-Specific Agencies, and non-Federal entities, including international entities, to carry out the cybersecurity and critical infrastructure activities of the Agency, as appropriate;

(3) carry out the responsibilities of the Secretary to secure Federal information and information systems consistent with law, including subchapter II of chapter 35 of title 44, United States Code, and the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113));

(4) coordinate a national effort to secure and protect against critical infrastructure risks, consistent with subsection (e)(1)(E);

(5) upon request, provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and, where appropriate, provide those analyses, expertise, and other technical assistance in coordination with Sector-Specific Agencies and other Federal departments and agencies;

(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;

[(6)**]** *(11)* develop and utilize mechanisms for active and frequent collaboration between the Agency and Sector-Specific Agencies to ensure appropriate coordination, situational awareness, and communications with Sector-Specific Agencies;

[(7)**]** *(12)* maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Divisions of the Agency to further operational coordination, inte-

grated situational awareness, and improved integration across the Agency in accordance with this Act;

[(8)] *(13)* develop, coordinate, and implement—

(A) comprehensive strategic plans for the activities of the Agency; and

(B) risk assessments by and for the Agency;

[(9)] *(14)* carry out emergency communications responsibilities, in accordance with title XVIII;

[(10)] *(15)* carry out cybersecurity, infrastructure security, and emergency communications stakeholder outreach and engagement and coordinate that outreach and engagement with critical infrastructure Sector-Specific Agencies, as appropriate; and

[(11)] *(16)* carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) DEPUTY DIRECTOR.—There shall be in the Agency a Deputy Director of Cybersecurity and Infrastructure Security who shall—

(1) assist the Director in the management of the Agency; and

(2) report to the Director.

(e) CYBERSECURITY AND INFRASTRUCTURE SECURITY AUTHORITIES OF THE SECRETARY.—

(1) IN GENERAL.—The responsibilities of the Secretary relating to cybersecurity and infrastructure security shall include the following:

(A) To access, receive, and analyze law enforcement information, intelligence information, and other information from Federal Government agencies, State, local, tribal, and territorial government agencies, including law enforcement agencies, and private sector entities, and to integrate that information, in support of the mission responsibilities of the Department, in order to—

(i) identify and assess the nature and scope of terrorist threats to the homeland;

(ii) detect and identify threats of terrorism against the United States; and

(iii) understand those threats in light of actual and potential vulnerabilities of the homeland.

(B) To carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States, including an assessment of the probability of success of those attacks and the feasibility and potential efficacy of various countermeasures to those attacks. At the discretion of the Secretary, such assessments may be carried out in coordination with Sector-Specific Agencies.

(C) To integrate relevant information, analysis, and vulnerability assessments, regardless of whether the information, analysis, or assessments are provided or produced by the Department, in order to make recommendations, including prioritization, for protective and support measures by the Department, other Federal Government agencies, State, local, tribal, and territorial government agencies

and authorities, the private sector, and other entities regarding terrorist and other threats to homeland security.

(D) To ensure, pursuant to section 202, the timely and efficient access by the Department to all information necessary to discharge the responsibilities under this title, including obtaining that information from other Federal Government agencies.

(E) To develop, in coordination with the Sector-Specific Agencies with available expertise, a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems, emergency communications systems, and the physical and technological assets that support those systems.

(F) To recommend measures necessary to protect the key resources and critical infrastructure of the United States in coordination with other Federal Government agencies, including Sector-Specific Agencies, and in cooperation with State, local, tribal, and territorial government agencies and authorities, the private sector, and other entities.

(G) To review, analyze, and make recommendations for improvements to the policies and procedures governing the sharing of information relating to homeland security within the Federal Government and between Federal Government agencies and State, local, tribal, and territorial government agencies and authorities.

(H) To disseminate, as appropriate, information analyzed by the Department within the Department to other Federal Government agencies with responsibilities relating to homeland security and to State, local, tribal, and territorial government agencies and private sector entities with those responsibilities in order to assist in the deterrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

(I) To consult with State, local, tribal, and territorial government agencies and private sector entities to ensure appropriate exchanges of information, including law enforcement-related information, relating to threats of terrorism against the United States.

(J) To ensure that any material received pursuant to this Act is protected from unauthorized disclosure and handled and used only for the performance of official duties.

(K) To request additional information from other Federal Government agencies, State, local, tribal, and territorial government agencies, and the private sector relating to threats of terrorism in the United States, or relating to other areas of responsibility assigned by the Secretary, including the entry into cooperative agreements through the Secretary to obtain such information.

(L) To establish and utilize, in conjunction with the Chief Information Officer of the Department, a secure com-

munications and information technology infrastructure, including data-mining and other advanced analytical tools, in order to access, receive, and analyze data and information in furtherance of the responsibilities under this section, and to disseminate information acquired and analyzed by the Department, as appropriate.

(M) To coordinate training and other support to the elements and personnel of the Department, other Federal Government agencies, and State, local, tribal, and territorial government agencies that provide information to the Department, or are consumers of information provided by the Department, in order to facilitate the identification and sharing of information revealed in their ordinary duties and the optimal utilization of information received from the Department.

(N) To coordinate with Federal, State, local, tribal, and territorial law enforcement agencies, and the private sector, as appropriate.

(O) To exercise the authorities and oversight of the functions, personnel, assets, and liabilities of those components transferred to the Department pursuant to section 201(g).

(P) To carry out the functions of the national cybersecurity and communications integration center under section 2209.

(Q) To carry out the requirements of the Chemical Facility Anti-Terrorism Standards Program established under title XXI and the secure handling of ammonium nitrate program established under subtitle J of title VIII, or any successor programs.

(2) REALLOCATION.—The Secretary may reallocate within the Agency the functions specified in sections 2203(b) and 2204(b), consistent with the responsibilities provided in paragraph (1), upon certifying to and briefing the appropriate congressional committees, and making available to the public, at least 60 days prior to the reallocation that the reallocation is necessary for carrying out the activities of the Agency.

(3) STAFF.—

(A) IN GENERAL.—The Secretary shall provide the Agency with a staff of analysts having appropriate expertise and experience to assist the Agency in discharging the responsibilities of the Agency under this section.

(B) PRIVATE SECTOR ANALYSTS.—Analysts under this subsection may include analysts from the private sector.

(C) SECURITY CLEARANCES.—Analysts under this subsection shall possess security clearances appropriate for their work under this section.

(4) DETAIL OF PERSONNEL.—

(A) IN GENERAL.—In order to assist the Agency in discharging the responsibilities of the Agency under this section, personnel of the Federal agencies described in subparagraph (B) may be detailed to the Agency for the performance of analytic functions and related duties.

(B) AGENCIES.—The Federal agencies described in this subparagraph are—

(i) the Department of State;

(ii) the Central Intelligence Agency;
(iii) the Federal Bureau of Investigation;
(iv) the National Security Agency;
(v) the National Geospatial-Intelligence Agency;
(vi) the Defense Intelligence Agency;
(vii) Sector-Specific Agencies; and
(viii) any other agency of the Federal Government that the President considers appropriate.

(C) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal agency described in subparagraph (B) may enter into agreements for the purpose of detailing personnel under this paragraph.

(D) BASIS.—The detail of personnel under this paragraph may be on a reimbursable or non-reimbursable basis.

(f) COMPOSITION.—The Agency shall be composed of the following divisions:

(1) The Cybersecurity Division, headed by an Assistant Director.

(2) The Infrastructure Security Division, headed by an Assistant Director.

(3) The Emergency Communications Division under title XVIII, headed by an Assistant Director.

(g) CO-LOCATION.—

(1) IN GENERAL.—To the maximum extent practicable, the Director shall examine the establishment of central locations in geographical regions with a significant Agency presence.

(2) COORDINATION.—When establishing the central locations described in paragraph (1), the Director shall coordinate with component heads and the Under Secretary for Management to co-locate or partner on any new real property leases, renewing any occupancy agreements for existing leases, or agreeing to extend or newly occupy any Federal space or new construction.

(h) PRIVACY.—

(1) IN GENERAL.—There shall be a Privacy Officer of the Agency with primary responsibility for privacy policy and compliance for the Agency.

(2) RESPONSIBILITIES.—The responsibilities of the Privacy Officer of the Agency shall include—

(A) assuring that the use of technologies by the Agency sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information;

(B) assuring that personal information contained in systems of records of the Agency is handled in full compliance as specified in section 552a of title 5, United States Code (commonly known as the "Privacy Act of 1974");

(C) evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Agency; and

(D) conducting a privacy impact assessment of proposed rules of the Agency on the privacy of personal information, including the type of personal information collected and the number of people affected.

(i) SAVINGS.—Nothing in this title may be construed as affecting in any manner the authority, existing on the day before the date

of enactment of this title, of any other component of the Department or any other Federal department or agency, including the authority provided to the Sector-Specific Agency specified in section 61003(c) of division F of the Fixing America's Surface Transportation Act (6 U.S.C. 121 note; Public Law 114–94).

* * * * * * *

SEC. 2210. CYBERSECURITY PLANS.

(a) DEFINITIONS.—In this section—

(1) the term "agency information system" means an information system used or operated by an agency or by another entity on behalf of an agency;

(2) the terms "cybersecurity risk" and "information system" have the meanings given those terms in section 2209;

(3) the term "intelligence community" has the meaning given the term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)); and

(4) the term "national security system" has the meaning given the term in section 11103 of title 40, United States Code.

(b) INTRUSION ASSESSMENT PLAN.—

(1) REQUIREMENT.—The Secretary, in coordination with the Director of the Office of Management and Budget, shall—

(A) develop and implement an intrusion assessment plan to proactively detect, identify, and remove intruders in agency information systems on a routine basis; and

(B) update such plan as necessary.

(2) EXCEPTION.—The intrusion assessment plan required under paragraph (1) shall not apply to the Department of Defense, a national security system, or an element of the intelligence community.

(c) CYBER INCIDENT RESPONSE PLAN.—The Director of Cybersecurity and InfrastructureSecurity shall, in coordination with appropriate Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 2222(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 2209) to critical infrastructure.

(d) NATIONAL RESPONSE FRAMEWORK.—The Secretary, in coordination with the heads of other appropriate Federal departments and agencies, and in accordance with the National Cybersecurity Incident Response Plan required under subsection (c), shall regularly update, maintain, and exercise the Cyber Incident Annex to the National Response Framework of the Department.

(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.

* * * * * * *

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 prac-

tices 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; and

(ii) 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).

* * * * * * *

○