117TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
117–48

STATE AND LOCAL CYBERSECURITY IMPROVEMENT ACT

JUNE 1, 2021.—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. 3138]

The Committee on Homeland Security, to whom was referred the bill (H.R. 3138) to amend the Homeland Security Act of 2002 to authorize a grant program relating to the cybersecurity of State and local 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

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. 2220A. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

"(a) DEFINITIONS.—In this section:

"(1) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given the term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

"(2) CYBERSECURITY PLAN.—The term 'Cybersecurity Plan' means a plan submitted by an eligible entity under subsection (e)(1).

"(3) ELIGIBLE ENTITY.—The term 'eligible entity' means—

"(A) a State; or

"(B) an Indian tribe that, 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—

"(i) notifies the Secretary that the Indian tribe intends to develop a Cybersecurity Plan; and

"(ii) agrees to forfeit any distribution under subsection (n)(2).

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

"(5) INDIAN TRIBE; TRIBAL ORGANIZATION.—The term 'Indian tribe' or 'Tribal organization' has the meaning given that term in section 4(e) of the of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304(e)).

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

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

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

"(9) RANSOMWARE INCIDENT.—The term 'ransomware incident' means an incident that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system for the purpose of coercing the information system's owner, operator, or another person.

"(9) STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The term 'State and Local Cybersecurity Grant Program' means the program established under subsection (b).

"(10) STATE AND LOCAL CYBERSECURITY RESILIENCE COMMITTEE.—The term 'State and Local Cybersecurity Resilience Committee' means the committee established under subsection (o)(1).

"(b) ESTABLISHMENT.—

"(1) IN GENERAL.—The Secretary, acting through the Director, shall establish a program, to be known as the 'the State and Local Cybersecurity Grant Program', to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations.

"(2) APPLICATION.—An eligible entity seeking a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

"(c) BASELINE REQUIREMENTS.—An eligible entity or multistate group that receives a grant under this section shall use the grant in compliance with—

"(1)(A) the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group; and

"(B) the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments developed under section 2210(e)(1); or

"(2) activities carried out under paragraphs (3), (4), and (5) of subsection (h).

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

"(e) CYBERSECURITY PLANS.—

"(1) IN GENERAL.—An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for approval.

"(2) REQUIRED ELEMENTS.—A Cybersecurity Plan of an eligible entity shall—

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

"(B) describe, to the extent practicable, how the eligible entity will—

"(i) manage, monitor, and track information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

"(ii) monitor, audit, and track activity between information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and between those information systems and information systems not owned or operated by the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity;

"(iii) enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or local or Tribal organizations against cybersecurity risks and cybersecurity threats;

"(iv) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems of the eligible entity or local or Tribal organizations;

"(v) ensure that State, local, and Tribal organizations that own or operate information systems that are located within the jurisdiction of the eligible entity—

"(I) adopt best practices and methodologies to enhance cybersecurity, such as the practices set forth in the cybersecurity framework developed by, and the cyber supply chain risk management best practices identified by, the National Institute of Standards and Technology; and

"(II) utilize knowledge bases of adversary tools and tactics to assess risk;

"(vi) promote the delivery of safe, recognizable, and trustworthy online services by State, local, and Tribal organizations, including through the use of the .gov internet domain;

"(vii) ensure continuity of operations of the eligible entity and local, and Tribal organizations in the event of a cybersecurity incident (including a ransomware incident), including by conducting exercises to practice responding to such an incident;

"(viii) use the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of State, local, or Tribal organizations, enhance recruitment and retention efforts for such workforces, and bolster the knowledge, skills, and abilities of State, local, and Tribal organization personnel to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

"(ix) ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the eligible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity in the event of an incident involving such communications or data networks within the jurisdiction of the eligible entity;

"(x) 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 the jurisdiction of the eligible entity;

"(xi) enhance capabilities to share cyber threat indicators and related information between the eligible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity, including by expanding existing information sharing agreements with the Department;

"(xii) enhance the capability of the eligible entity to share cyber threat indictors and related information with the Department;

"(xiii) leverage cybersecurity services offered by the Department;

"(xiv) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats to information systems of the eligible entity in consultation with—

"(I) local and Tribal organizations within the jurisdiction of the eligible entity; and

"(II) as applicable—

"(aa) States that neighbor the jurisdiction of the eligible entity or, as appropriate, members of an information sharing and analysis organization; and

"(bb) countries that neighbor the jurisdiction of the eligible entity; and

"(xv) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

"(C) describe, to the extent practicable, the individual responsibilities of the eligible entity and local and Tribal organizations within the jurisdiction of the eligible entity in implementing the plan;

"(D) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

"(E) describe how the eligible entity will measure progress towards implementing the plan.

"(3) DISCRETIONARY ELEMENTS.—A Cybersecurity Plan of an eligible entity may include a description of—

"(A) cooperative programs developed by groups of local and Tribal organizations within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

"(B) programs provided by the eligible entity to support local and Tribal organizations and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

"(4) MANAGEMENT OF FUNDS.—An eligible entity applying for a grant under this section shall agree to designate the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity as the primary official for the management and allocation of funds awarded under this section.

"(f) MULTISTATE GRANTS.—

"(1) IN GENERAL.—The Secretary, acting through the Director, may award grants under this section to a group of two or more eligible entities to support multistate efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities.

"(2) SATISFACTION OF OTHER REQUIREMENTS.—In order to be eligible for a multistate grant under this subsection, each eligible entity that comprises a multistate group shall submit to the Secretary—

"(A) a Cybersecurity Plan for approval in accordance with subsection (i); and

"(B) a plan for establishing a cybersecurity planning committee under subsection (g).

"(3) APPLICATION.—

"(A) IN GENERAL.—A multistate group applying for a multistate grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

"(B) MULTISTATE PROJECT DESCRIPTION.—An application of a multistate group under subparagraph (A) shall include a plan describing—

"(i) the division of responsibilities among the eligible entities that comprise the multistate group for administering the grant for which application is being made;

"(ii) the distribution of funding from such a grant among the eligible entities that comprise the multistate group; and

"(iii) how the eligible entities that comprise the multistate group will work together to implement the Cybersecurity Plan of each of those eligible entities.

"(g) PLANNING COMMITTEES.—

"(1) IN GENERAL.—An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

"(A) assist in the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

"(B) approve the Cybersecurity Plan of the eligible entity; and

"(C) assist in the determination of effective funding priorities for a grant under this section in accordance with subsection (h).

"(2) COMPOSITION.—A committee of an eligible entity established under paragraph (1) shall—

"(A) be comprised of representatives from the eligible entity and counties, cities, towns, Tribes, and public educational and health institutions within the jurisdiction of the eligible entity; and

"(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

"(3) CYBERSECURITY EXPERTISE.—Not less than ½ of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

"(4) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMITTEES.—Nothing in this subsection may be construed to require an eligible entity to establish a cybersecurity planning committee if the eligible entity has established and uses a multijurisdictional planning committee or commission that meets, or may be leveraged to meet, the requirements of this subsection.

"(h) USE OF FUNDS.—An eligible entity that receives a grant under this section shall use the grant to—

"(1) implement the Cybersecurity Plan of the eligible entity;

"(2) develop or revise the Cybersecurity Plan of the eligible entity; or

"(3) assist with activities that address imminent cybersecurity risks or cybersecurity threats to the information systems of the eligible entity or a local or Tribal organization within the jurisdiction of the eligible entity.

"(i) APPROVAL OF PLANS.—

"(1) APPROVAL AS CONDITION OF GRANT.—Before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall review the Cybersecurity Plan, or any revisions thereto, of the eligible entity and approve such plan, or revised plan, if it satisfies the requirements specified in paragraph (2).

"(2) PLAN REQUIREMENTS.—In approving a Cybersecurity Plan of an eligible entity under this subsection, the Director shall ensure that the Cybersecurity Plan—

"(A) satisfies the requirements of subsection (e)(2);

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

"(C) has been approved by the cybersecurity planning committee of the eligible entity established under subsection (g).

"(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 subsection (e) and paragraph (1) of this subsection, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary if—

"(A) the eligible entity certifies to the Secretary that—

"(i) the activities that will be supported by the grant are integral to the development of the Cybersecurity Plan of the eligible entity; and

"(ii) the eligible entity will submit by September 30, 2023, to the Secretary a Cybersecurity Plan for review, and if appropriate, approval; or

"(B) the eligible entity certifies to the Secretary, and the Director confirms, that the eligible entity will use funds from the grant to assist with the activities described in subsection (h)(3).

"(j) LIMITATIONS ON USES OF FUNDS.—

"(1) IN GENERAL.—An eligible entity that receives a grant under this section may not use the grant—

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

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

"(C) to pay a demand for ransom in an attempt to—

"(i) regain access to information or an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity; or

"(ii) prevent the disclosure of information that has been removed without authorization from an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity;

"(D) for recreational or social purposes; or

"(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity.

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

"(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1) may be construed to prohibit the use of grant funds provided to a State, local, or Tribal organization for otherwise permissible uses under this section on the basis that a State, local, or Tribal organization has previously used State, local, or Tribal funds to support the same or similar uses.

"(k) 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.

"(l) APPORTIONMENT.—For fiscal year 2022 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, the U.S. 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 eligible entity, bears to

"(B) the population of all eligible entities.

"(3) MINIMUM ALLOCATION TO INDIAN TRIBES.—

"(A) IN GENERAL.—In apportioning amounts under this section, the Secretary shall ensure that, for each fiscal year, directly eligible Tribes collectively receive, from amounts appropriated under the State and Local Cybersecurity Grant Program, not less than an amount equal to three percent of the total amount appropriated for grants under this section.

"(B) ALLOCATION.—Of the amount reserved under subparagraph (A), funds shall be allocated in a manner determined by the Secretary in consultation with Indian tribes.

"(C) EXCEPTION.—This paragraph shall not apply in any fiscal year in which the Secretary—

"(i) receives fewer than five applications from Indian tribes; or

"(ii) does not approve at least two application from Indian tribes.

"(m) FEDERAL SHARE.—

"(1) IN GENERAL.—The Federal share of the cost of an activity carried out using funds made available with a grant under this section may not exceed—

"(A) in the case of a grant to an eligible entity—

"(i) for fiscal year 2022, 90 percent;

"(ii) for fiscal year 2023, 80 percent;

"(iii) for fiscal year 2024, 70 percent;

"(iv) for fiscal year 2025, 60 percent; and

"(v) for fiscal year 2026 and each subsequent fiscal year, 50 percent; and

"(B) in the case of a grant to a multistate group—

"(i) for fiscal year 2022, 95 percent;

"(ii) for fiscal year 2023, 85 percent;

"(iii) for fiscal year 2024, 75 percent;

"(iv) for fiscal year 2025, 65 percent; and

"(v) for fiscal year 2026 and each subsequent fiscal year, 55 percent.

"(2) WAIVER.—The Secretary may waive or modify the requirements of paragraph (1) for an Indian tribe if the Secretary determines such a waiver is in the public interest.

"(n) RESPONSIBILITIES OF GRANTEES.—

"(1) CERTIFICATION.—Each eligible entity or multistate group that receives a grant under this section shall certify to the Secretary that the grant will be used—

"(A) for the purpose for which the grant is awarded; and

"(B) in compliance with, as the case may be—

"(i) the Cybersecurity Plan of the eligible entity;

"(ii) the Cybersecurity Plans of the eligible entities that comprise the multistate group; or

"(iii) a purpose approved by the Secretary under subsection (h) or pursuant to an exception under subsection (i).

"(2) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL ORGANIZATIONS.—Not later than 45 days after the date on which an eligible entity or multistate group receives a grant under this section, the eligible entity or multistate group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local and Tribal organizations within the jurisdiction of the eligible entity or the eligible entities that comprise the multistate group, and as applicable, consistent with the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group—

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

"(B) with the consent of the local and Tribal organizations, 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 and Tribal organizations, 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 AND TRIBAL ORGANIZATIONS.—An eligible entity or multistate group shall certify to the Secretary that the eligible entity or multistate group has made the distribution to local, Tribal, and territorial governments required under paragraph (2).

"(4) EXTENSION OF PERIOD.—

"(A) IN GENERAL.—An eligible entity or multistate group may request in writing that the Secretary extend the period of time specified in paragraph (2) for an additional period of time.

"(B) APPROVAL.—The Secretary may approve a request for an extension under subparagraph (A) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the purpose of the State and Local Cybersecurity 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, the Virgin Islands, or an Indian tribe.

"(6) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local or Tribal organization required in accordance with paragraph (2), the local or Tribal organization may petition the Secretary to request that grant funds be provided directly to the local or Tribal organization.

"(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 an eligible entity or distribute grant funds previously awarded to such eligible entity directly to the appropriate local or Tribal organization as a replacement grant in an amount the Secretary determines appropriate if such eligible entity violates a requirement of this subsection.

"(o) ADVISORY COMMITTEE.—

"(1) ESTABLISHMENT.—Not later than 120 days after the date of enactment of this section, the Director shall establish a State and Local Cybersecurity Resilience Committee to provide State, local, and Tribal 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, or Tribal organizations; and

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

"(2) DUTIES.—The committee established under paragraph (1) 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 those plans prior to the approval of the plans under subsection (i);

"(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;

"(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, or Tribal organizations; and

"(ii) improve the cybersecurity resilience of State, local, or Tribal organizations; and

"(E) regularly coordinate with the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

"(3) MEMBERSHIP.—

"(A) NUMBER AND APPOINTMENT.—The State and Local Cybersecurity Resilience Committee established pursuant to paragraph (1) 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) One individual 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) One individual recommended to the Director by the National Congress of American Indians.

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

"(B) TERMS.—

"(i) IN GENERAL.—Subject to clause (ii), each member of the State and Local Cybersecurity Resilience Committee shall be appointed for a term of two years.

"(ii) REQUIREMENT.—At least two members of the State and Local Cybersecurity Resilience Committee shall also be members of the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

"(iii) EXCEPTION.—A term of a member of the State and Local Cybersecurity Resilience Committee shall be three years if the member is appointed initially to the Committee upon the establishment of the Committee.

"(iv) TERM REMAINDERS.—Any member of the State and Local Cybersecurity Resilience Committee 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.

"(v) VACANCIES.—A vacancy in the State and Local Cybersecurity Resilience Committee shall be filled in the manner in which the original appointment was made.

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

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

"(5) PERMANENT AUTHORITY.—Notwithstanding section 14 of the Federal Advisory Committee Act (5 U.S.C. App.), the State and Local Cybersecurity Resilience Committee shall be a permanent authority.

"(p) REPORTS.—

"(1) ANNUAL REPORTS BY GRANT RECIPIENTS.—

"(A) IN GENERAL.—Not later than one year after an eligible entity or multistate group receives funds under this section, the eligible entity or multistate group shall submit to the Secretary a report on the progress of the eligible entity or multistate group in implementing the Cybersecurity Plan of the eligible entity or Cybersecurity Plans of the eligible entities that comprise the multistate group, as the case may be.

"(B) ABSENCE OF PLAN.—Not later than 180 days after an eligible entity that does not have a Cybersecurity Plan receives funds under this section for developing its Cybersecurity Plan, the eligible entity shall submit to the

Secretary a report describing how the eligible entity obligated and expended grant funds during the fiscal year to—

"(i) so develop such a Cybersecurity Plan; or

"(ii) assist with the activities described in subsection (h)(3).

"(2) ANNUAL REPORTS TO CONGRESS.—Not less frequently than once per 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 date on which the strategy is issued under section 2210.

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

"(C) Reducing cybersecurity risks and cybersecurity threats to information systems, applications, and user accounts owned or operated by or on behalf of State, local, and Tribal organizations as a result of the award of such grants.

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

"(1) for each of fiscal years 2022 through 2026, $500,000,000; and

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

"SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOPMENT FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT OFFICIALS.

"The Secretary, acting through the Director, shall develop, regularly update, and maintain 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 (as such term is defined in section 2209), 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, as amended by section 4, is further amended by inserting after the item relating to section 2220 the following new items:

"Sec. 2220A. State and Local Cybersecurity Grant Program.
"Sec. 2220B. 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.—

"(A) REQUIREMENT.—Not later than one year after the date of the enactment of this subsection, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee established under section 2220A, 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.

"(B) RECOMMENDATIONS AND REQUIREMENTS.—The strategy required under subparagraph (A) shall—

"(i) provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks (as such term is defined in section 2209), cybersecurity threats, and incidents (as such term is defined in section 2209); and

"(ii) establish baseline requirements for cybersecurity plans under this section and principles with which such plans shall align.

"(2) CONTENTS.—The strategy 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, incidents, and ransomware incidents;

"(B) identify Federal resources and capabilities that are available or could be made available to State, local, Tribal, and territorial governments to

help those governments identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

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

"(D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve—

"(i) incident exercises, information sharing and incident notification procedures;

"(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

"(iii) 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 identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

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

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

"(3) CONSIDERATIONS.—In developing the strategy required under paragraph (1), the Director, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee established under section 2220A, 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 (as such term is defined in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)) 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 established under section 2220A.

"(4) EXEMPTION.—Chapter 35 of title 44, United States Code (commonly known as the 'Paperwork Reduction Act'), shall not apply to any action to implement this subsection.".

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

(1) by redesignating subsections (d) through (i) as subsections (e) through (j), respectively; and

(2) by inserting after subsection (c) the following new subsection:

"(d) ADDITIONAL RESPONSIBILITIES.—In addition to the responsibilities under subsection (c), the Director shall—

"(1) develop program guidance, in consultation with the State and Local Government Cybersecurity Resilience Committee established under section 2220A, for the State and Local Cybersecurity Grant Program under such section or any other homeland security assistance administered by the Department to improve cybersecurity;

"(2) review, in consultation with the State and Local Cybersecurity Resilience Committee, all cybersecurity plans of State, local, Tribal, and territorial govern-

ments developed pursuant to any homeland security assistance administered by the Department to improve cybersecurity;

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

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

(c) FEASIBILITY STUDY.—Not later than 270 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security of the Department of Homeland Security shall conduct a study to assess the feasibility of implementing a short-term rotational program for the detail to the Agency of approved State, local, Tribal, and territorial government employees in cyber workforce positions.

SEC. 4. TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.

(a) TECHNICAL AMENDMENTS.—

(1) HOMELAND SECURITY ACT OF 2002.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(A) in the first section 2215 (6 U.S.C. 665; relating to the duties and authorities relating to .gov internet domain), by amending the section enumerator and heading to read as follows:

"SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.";

(B) in the second section 2215 (6 U.S.C. 665b; relating to the joint cyber planning office), by amending the section enumerator and heading to read as follows:

"SEC. 2216. JOINT CYBER PLANNING OFFICE.";

(C) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

"SEC. 2217. CYBERSECURITY STATE COORDINATOR.";

(D) in the fourth section 2215 (6 U.S.C. 665d; relating to Sector Risk Management Agencies), by amending the section enumerator and heading to read as follows:

"SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.";

(E) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

"SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE."; and

(F) in section 2217 (6 U.S.C. 665f; relating to Cybersecurity Education and Training Programs), by amending the section enumerator and heading to read as follows:

"SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.".

(2) CONSOLIDATED APPROPRIATIONS ACT, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter preceding subparagraph (A), by inserting "of 2002" after "Homeland Security Act".

(b) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 2214 through 2217 and inserting the following new items:

"Sec. 2214. National Asset Database.
"Sec. 2215. Duties and authorities relating to .gov internet domain.
"Sec. 2216. Joint cyber planning office.
"Sec. 2217. Cybersecurity State Coordinator.
"Sec. 2218. Sector Risk Management Agencies.
"Sec. 2219. Cybersecurity Advisory Committee.
"Sec. 2220. Cybersecurity Education and Training Programs.".

PURPOSE AND SUMMARY

H.R. 3138, the "State and Local Cybersecurity Act," seeks to foster stronger partnerships between the Federal government and State and local governments to defend State and local networks against cyber attacks from sophisticated foreign adversaries or cyber criminals. It does so by authorizing a new Department of Homeland Security (DHS) grant program to address cybersecurity vulnerabilities on State and local government networks. This new

$500 million grant program includes a graduating cost-share to incentivize 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 a short-term rotational program for certain cybersecurity professionals in State, local, Tribal, and Territorial workforces to be detailed to the Agency. Lastly, H.R. 3138 establishes a State and Local Cybersecurity Resilience 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 service disruptions and system failures would impose. However, State and local agencies often have far fewer resources and cybersecurity personnel than their Federal counterparts or similarly sized private sector entities.

At the State level, cybersecurity responsibilities are generally carried out by a Chief Information Security Officer (CISO). In a survey as part of the National Association of State Chief Information Security Officers' (NASCIO) *2020 Cybersecurity Study*, CISOs overwhelmingly report a lack of a sufficient, reliable budgets to develop their statewide security program. In most States, cybersecurity funding is derived from the State's IT budget and is not designated as a separate line item. Further, the percentage of State enterprise IT budgets allocated to enterprise cybersecurity is only 1–3 percent—far lower than the Federal government or private industries, such as the financial services sector, which spends 10.9 percent of its IT budget on cybersecurity.

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 percent of local government Chief Information Officers (CIOs) reported having experienced an attack during the last 12 months, and 26 percent reported an attack, incident, or breach attempt occurring hourly. At the same time, many local governments are not well prepared to recover from a ransomware attack, detect or prevent exfiltration, recover from breaches, or detect attacks. Moreover, many local officials and staff are not sufficiently aware of the need for cybersecurity.

According to an August 2020 report issued by cybersecurity firm BlueVoyant, cyber attacks against State and local governments rose 50 percent between 2017 and 2020. Most attacks were not complicated, but rather could be prevented by improved cyber hygiene and adoption of multifactor authentication. In 2018, devastating ransomware attacks crippled Atlanta, Georgia. The fol-

lowing year, ransomware attacks disrupted State and local agencies in Louisiana; the City of Baltimore, Maryland; 22 towns in Texas; a school district in Syracuse, New York; and many other communities across the country. In a growing number of ransomware attacks, the perpetrators engage in "double extortion" where they threaten to release sensitive data publicly if a ransom payment is not made. In April 2021, the Washington, DC, police department was hit by a ransomware attack that included the release of detailed background reports on multiple current or former police officers and the threat to release files related to police informants. 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." 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.

Stretched State and local budgets have not adequately funded cybersecurity, and the emergence of the COVID–19 pandemic in 2020 further highlighted existing cybersecurity challenges at the State and local level. According to the Brookings Institution, by April 2020, the pandemic led to, "up to half of American workers [. . .] working from home." 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.

To address this urgent national security issue, the Federal government needs to redouble its efforts to partner 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 authorizes funding to ensure those strategies are implemented. Investing in cybersecurity before a cyber attack 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. 3138 has been endorsed by NASCIO. Additionally, on May 20, 2021, the following groups urged that H.R. 3138 be included in any infrastructure package advanced by Congress: Rapid7, Alliance for Digital Innovation, Avast, Broadcom, Bugcrowd, Citrix, Cybereason, Cybersecurity Coalition, Cyber Threat Alliance, Disclose.io, Global Cyber Alliance, GRIMM, ICS Village, Institute for Security and Technology, Luta, McAfee, SCYTHE, Security Scorecard, and Tenable.

A similar measure, H.R. 5823, passed the House of Representatives in the 116th Congress by voice vote on September 30, 2020.

HEARINGS

For the purposes of clause 3(c)(6) of rule XIII, the following hearings were used to develop H.R. 3138:

The Committee did not hold a legislative hearing on H.R. 3138 in the 117th Congress. However, the legislation was informed by several oversight hearings.

On February 10, 2021, the Full Committee held a hearing entitled, "Homeland Cybersecurity: Assessing Cyber Threats and Building Resilience." The following witnesses testified: Susan Gordon, former Principal Deputy Director of National Intelligence, Office of the Director of National Intelligence; Christopher Krebs, former Director, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security; Michael Daniel, President & CEO, Cyber Threat Alliance, former White House Cybersecurity Coordinator; and Dmitri Alperovitch, Executive Chairman, Silverado Policy Accelerator.

On April 28, 2021, the Subcommittee on Emergency Preparedness, Response, and Resilience held a hearing entitled, "State and Local on DHS Preparedness Grant Programs." The following witnesses testified: The Honorable David Ige, Governor, Hawaii; Jared Maples, Director, New Jersey Office of Homeland Security and Preparedness; Orlando Rolón, Police Chief, City of Orlando, Florida; Robert Altman, Battalion Chief, Ocala Fire Rescue.

On May 5, 2021, the Subcommittee on Cybersecurity, Infrastructure Protection, and Innovation held a hearing entitled, "Responding to Ransomware: Exploring Policy Solutions to a Cybersecurity Crisis." The following witnesses testified: Maj. Gen. John Davis (Ret.), Vice President and Federal Chief Security Officer at Palo Alto Networks; Megan Stifel, Executive Director, Americas at the Global Cyber Alliance; Denis Goulet, Commissioner, Department of Information Technology and Chief Information Officer, State of New Hampshire (on behalf of the National Association of State Chief Information Officers); and Christopher Krebs, former Director, Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security.

COMMITTEE CONSIDERATION

The Committee met on May 18, 2021, with a quorum being present, to consider H.R. 3138 and ordered the measure to be reported to the House with a favorable recommendation, as amended, by unanimous consent.

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. 3138.

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 the 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 has requested but not received from the Director of the Congressional Budget Office a statement as to whether this bill contains any new budget authority, spending authority, credit authority, or an increase or decrease in revenues or tax expenditures.

FEDERAL MANDATES STATEMENT

An estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act was not made available to the Committee in time for the filing of this report. The Chairman of the Committee shall cause such estimate to be printed in the Congressional Record upon its receipt by the Committee.

DUPLICATIVE FEDERAL PROGRAMS

Pursuant to clause 3(c) of rule XIII, the Committee finds that H.R. 3138 does not contain any provision that establishes or reauthorizes a program known to be duplicative of another Federal program.

STATEMENT OF GENERAL 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. 3138 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 Cybersecurity of State, Local, Tribal, and Territorial Governments" to which grantees can align their cybersecurity plans.

CONGRESSIONAL EARMARKS, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS ADVISORY COMMITTEE STATEMENT

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.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that H.R. 3138 does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

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 Improvement Act."

Sec. 2. State and Local Cybersecurity Grant Program.

Adds Sections 2220A and 2220B to Title XXII of the Homeland Security Act of 2002.

SECTION 2220A. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

(a) Definitions.—Provides definitions for "cyber threat indicator," "cybersecurity plan," "eligible entity," "incident," "Indian Tribe," "information sharing and analysis organization," "information system," "online service," "ransomware incident," "State and Local Cybersecurity Grant Program," and "State and Local Cybersecurity Resilience Committee."

(b) Establishment.—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 eligible entities (States, the District of Columbia, and U.S. Territories, as well as Federally recognized Tribes that elect to participate) to address cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or Territorial governments. The program will be referred to as the State and Local Cybersecurity Grant Program.

(c) Baseline Requirements.—Requires each eligible entity or multistate group receiving a grant under the State and Local Cybersecurity Grant Program to meet baseline requirements of complying with their Cybersecurity Plan and the "Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments."

(d) Administration.—Directs that the State and Local Cybersecurity Grant Program shall be administered by the same office that administers grants for the Urban Area Security Initiative and the State Homeland Security Grant Program.

(e) Cybersecurity Plans.—Requires each eligible entity applying for a grant to submit a Cybersecurity Plan and describes the required and discretionary elements of Cybersecurity Plans.

(f) Multistate Grants.—Allows grants to a group of two or more eligible entities to support multistate efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities. Each eligible entity must submit a Cybersecurity Plan and establish a cybersecurity planning committee, as otherwise required by the Act. A multistate group must further apply to the Secretary for a multistate grant and include a multistate project description that includes the division of responsibilities for administering the grant, the distribution of funding among the eligible entities, and how the eligible entities that comprise the multistate group with work together to implement the Cybersecurity Plan of each of those eligible entities.

(g) Planning Committees.—Requires each eligible entity receiving 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, Tribes, and public educational and health institutions within the eligible entity receiving a grant, including, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

(h) Use of Funds.—Describes the permissible use of funds awarded under the State and Local Cybersecurity Grant Program to include implementing an eligible entity's Cybersecurity Plan, developing or revising a Cybersecurity Plan, or to assist with activities that address imminent cybersecurity risks and cybersecurity threats to information systems of State, local, Tribal, or Territorial governments, as the case may be.

(i) Approval of Plans.—Requires the Secretary of Homeland Security, acting through the Director of the Cybersecurity and Infrastructure Agency, to review 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." Cybersecurity Plans must be approved by the Secretary before an eligible entity may receive grant funds, unless the eligible entity certifies that it will submit a Cybersecurity Plan by September 30, 2023, and grant funds will be used to develop the Cybersecurity Plan or the grant will address imminent cybersecurity risks or cybersecurity threats.

(j) Limitation on Uses of Funds.—Bars the use of 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 eligible entity or of a local or Tribal government in such eligible entity or to prevent disclosure of information removed without authorization; 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 eligible entity or of a local or Tribal government in such eligible entity. Eligible entities must certify that they will use grant dollars for an appropriate purpose. The Secretary is authorized to take such enforcement actions necessary.

(k) Opportunity to Amend Applications.—Authorizes eligible entities to amend grant applications to correct defects.

(l) Apportionment.—Sets forth the formula the Secretary shall use to apportion grant awards to eligible grantees. Three percent of the grant funds are reserved for Indian tribes.

(m) Federal Share.—Establishes a cost-share for eligible entities that increases over time to incentivize eligible entities to invest in cybersecurity. There is a lower cost share for multistate groups. The Secretary may waive cost share requirements for Indian tribes.

(n) Responsibilities of Grantees.—Requires States (but not Territories or Tribes) to make 80 percent of grant funds available to local and Tribal governments within 45 days of receiv-

ing the grant award, with certain exceptions. States must certify to the Secretary that it has made such distributions of grant awards. If a State fails to make funds available to local and Tribal governments, local and Tribal governments may seek direct funding from the Secretary. The Secretary may impose appropriate penalties to enforce this provision.

(o) Advisory Committee.—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 develop 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.

(p) Reports.—Requires eligible entities receiving a grant to annually submit to the Secretary of Homeland Security a report on the progress of the State in implementing the approved Cybersecurity Plan. If the eligible entity does not have an approved Cybersecurity Plan, the eligible entity 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 Committee expects the Secretary to establish a consistent 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. This section requires the Secretary of Homeland Security 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.

(q) Authorization of Appropriations.—Authorizes $500,000,000 in annual appropriations for this grant program from FY 2022 through FY 2026, and such sums necessary thereafter.

SEC. 2220B. CYBERSECURITY RESOURCES GUIDE DEVELOPMENT FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT OFFICIALS.

Requires the Secretary of Homeland Security, 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.

Sec. 3. Strategy.

(a) Homeland Security Strategy to Improve the Cybersecurity of State, Local Tribal, and Territorial Governments.—Requires that, not later than one year after the date of the enactment, 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, 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, mitigate against, 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 strategy is exempt from the requirements of the Paperwork Reduction Act.

(b) Responsibilities of the Director of the Cybersecurity and Infrastructure Security Agency.—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.

(c) Feasibility Study.—Requires the Director of the Cybersecurity and Infrastructure Security Agency to, not later than 260 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.

Sec. 4. Title XXII Technical and Clerical Amendments.

This section makes technical corrections to the section enumerators of title XXII of the Homeland Security Act of 2002.

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:

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) QUALIFICATIONS.—

(A) IN GENERAL.—The Director shall be appointed from among individuals who have—

(i) extensive knowledge in at least two of the areas specified in subparagraph (B); and

(ii) not fewer than five years of demonstrated experience in efforts to foster coordination and collaboration between the Federal Government, the private sector, and other entities on issues related to cybersecurity, infrastructure security, or security risk management.

(B) SPECIFIED AREAS.—The areas specified in this subparagraph are the following:

(i) Cybersecurity.

(ii) Infrastructure security.

(iii) Security risk management.

(3) REFERENCE.—Any reference to an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, 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 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) maintain and utilize mechanisms for the regular and ongoing consultation and collaboration among the Divisions of the Agency to further operational coordination, integrated situational awareness, and improved integration across the Agency in accordance with this Act;

(8) develop, coordinate, and implement—

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

(B) risk assessments by and for the Agency;

(9) carry out emergency communications responsibilities, in accordance with title XVIII;

(10) 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;

(11) provide education, training, and capacity development to Federal and non-Federal entities to enhance the security and resiliency of domestic and global cybersecurity and infrastructure security; and

(12) appoint a Cybersecurity State Coordinator in each State, as described in section 2215; and

(12) carry out the duties and authorities relating to the.gov internet domain, as described in section 2215; and

(12) carry out such other duties and powers prescribed by law or delegated by the Secretary.

(d) ADDITIONAL RESPONSIBILITIES.—In addition to the responsibilities under subsection (c), the Director shall—

(1) develop program guidance, in consultation with the State and Local Government Cybersecurity Resilience Committee established under section 2220A, for the State and Local Cybersecurity Grant Program under such section or any other homeland security assistance administered by the Department to improve cybersecurity;

(2) review, in consultation with the State and Local Cybersecurity Resilience 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;

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

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

[(d)**]** *(e)* 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)**]** *(f)* 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 communications 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.

(R) To encourage and build cybersecurity awareness and competency across the United States and to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department, including by—

(i) overseeing elementary and secondary cybersecurity education and awareness related programs at the Agency;

(ii) leading efforts to develop, attract, and retain the cybersecurity workforce necessary for the cybersecurity related missions of the Department;

(iii) encouraging and building cybersecurity awareness and competency across the United States; and

(iv) carrying out cybersecurity related workforce development activities, including through—

(I) increasing the pipeline of future cybersecurity professionals through programs focused on elementary and secondary education, postsecondary education, and workforce development; and

(II) building awareness of and competency in cybersecurity across the civilian Federal Government workforce.

(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)] *(g)* 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)] *(h)* 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)] *(i)* 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)] *(j)* 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 Risk Management 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.—

(A) REQUIREMENT.—Not later than one year after the date of the enactment of this subsection, the Secretary, acting through the Director, shall, in coordination with the heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee established under section 2220A, 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.

(B) RECOMMENDATIONS AND REQUIREMENTS.—The strategy required under subparagraph (A) shall—

(i) provide recommendations relating to the ways in which the Federal Government should support and promote the ability of State, local, Tribal, and territorial governments to identify, mitigate against, protect against, detect, respond to, and recover from cybersecurity risks (as such term is defined in section 2209), cy-

bersecurity threats, and incidents (as such term is defined in section 2209); and

(ii) establish baseline requirements for cybersecurity plans under this section and principles with which such plans shall align.

(2) CONTENTS.—The strategy 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, incidents, and ransomware incidents;

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

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

(D) identify opportunities to improve the coordination of the Agency with Federal and non-Federal entities, such as the Multi-State Information Sharing and Analysis Center, to improve—

(i) incident exercises, information sharing and incident notification procedures;

(ii) the ability for State, local, Tribal, and territorial governments to voluntarily adapt and implement guidance in Federal binding operational directives; and

(iii) 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 identify, protect against, detect, respond to, and recover from cybersecurity risks, cybersecurity threats, incidents, and ransomware incidents;

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

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

(3) CONSIDERATIONS.—In developing the strategy required under paragraph (1), the Director, in coordination with the

heads of appropriate Federal agencies, State, local, Tribal, and territorial governments, the State and Local Cybersecurity Resilience Committee established under section 2220A, 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 (as such term is defined in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501)) 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 established under section 2220A.

(4) EXEMPTION.—Chapter 35 of title 44, United States Code (commonly known as the "Paperwork Reduction Act"), shall not apply to any action to implement this subsection.

* * * * * * *

SEC. 2215. DUTIES AND AUTHORITIES RELATING TO.GOV INTERNET DOMAIN.

(a) DEFINITION.—In this section, the term "agency" has the meaning given the term in section 3502 of title 44, United States Code.

(b) AVAILABILITY OF.GOV INTERNET DOMAIN.—The Director shall make.gov internet domain name registration services, as well as any supporting services described in subsection (e), generally available—

(1) to any Federal, State, local, or territorial government entity, or other publicly controlled entity, including any Tribal government recognized by the Federal Government or a State government, that complies with the requirements for registration developed by the Director as described in subsection (c);

(2) without conditioning registration on the sharing of any information with the Director or any other Federal entity, other than the information required to meet the requirements described in subsection (c); and

(3) without conditioning registration on participation in any separate service offered by the Director or any other Federal entity.

(c) REQUIREMENTS.—The Director, with the approval of the Director of the Office of Management and Budget for agency.gov internet domain requirements and in consultation with the Director of the Office of Management and Budget for.gov internet domain requirements for entities that are not agencies, shall establish and publish on a publicly available website requirements for the registration and operation of.gov internet domains sufficient to—

(1) minimize the risk of.gov internet domains whose names could mislead or confuse users;

(2) establish that.gov internet domains may not be used for commercial or political campaign purposes;

(3) ensure that domains are registered and maintained only by authorized individuals; and

(4) limit the sharing or use of any information obtained through the administration of the.gov internet domain with any other Department component or any other agency for any purpose other than the administration of the.gov internet domain, the services described in subsection (e), and the requirements for establishing a.gov inventory described in subsection (h).

(d) EXECUTIVE BRANCH.—

(1) IN GENERAL.—The Director of the Office of Management and Budget shall establish applicable processes and guidelines for the registration and acceptable use of.gov internet domains by agencies.

(2) APPROVAL REQUIRED.—The Director shall obtain the approval of the Director of the Office of Management and Budget before registering a.gov internet domain name for an agency.

(3) COMPLIANCE.—Each agency shall ensure that any website or digital service of the agency that uses a.gov internet domain is in compliance with the 21st Century IDEA Act (44 U.S.C. 3501 note) and implementation guidance issued pursuant to that Act.

(e) SUPPORTING SERVICES.—

(1) IN GENERAL.—The Director may provide services to the entities described in subsection (b)(1) specifically intended to support the security, privacy, reliability, accessibility, and speed of registered.gov internet domains.

(2) RULE OF CONSTRUCTION.—Nothing in paragraph (1) shall be construed to—

(A) limit other authorities of the Director to provide services or technical assistance to an entity described in subsection (b)(1); or

(B) establish new authority for services other than those the purpose of which expressly supports the operation of.gov internet domains and the needs of.gov internet domain registrants.

(f) FEES.—

(1) IN GENERAL.—The Director may provide any service relating to the availability of the.gov internet domain program, including.gov internet domain name registration services described in subsection (b) and supporting services described in subsection (e), to entities described in subsection (b)(1) with or without reimbursement, including variable pricing.

(2) LIMITATION.—The total fees collected for new.gov internet domain registrants or annual renewals of.gov internet domains shall not exceed the direct operational expenses of improving, maintaining, and operating the.gov internet domain,.gov internet domain services, and.gov internet domain supporting services.

(g) CONSULTATION.—The Director shall consult with the Director of the Office of Management and Budget, the Administrator of Gen-

eral Services, other civilian Federal agencies as appropriate, and entities representing State, local, Tribal, or territorial governments in developing the strategic direction of the.gov internet domain and in establishing requirements under subsection (c), in particular on matters of privacy, accessibility, transparency, and technology modernization.

(h) .GOV INVENTORY.—

(1) IN GENERAL.—The Director shall, on a continuous basis—

(A) inventory all hostnames and services in active use within the.gov internet domain; and

(B) provide the data described in subparagraph (A) to domain registrants at no cost.

(2) REQUIREMENTS.—In carrying out paragraph (1)—

(A) data may be collected through analysis of public and non-public sources, including commercial data sets;

(B) the Director shall share with Federal and non-Federal domain registrants all unique hostnames and services discovered within the zone of their registered domain;

(C) the Director shall share any data or information collected or used in the management of the.gov internet domain name registration services relating to Federal executive branch registrants with the Director of the Office of Management and Budget for the purpose of fulfilling the duties of the Director of the Office of Management and Budget under section 3553 of title 44, United States Code;

(D) the Director shall publish on a publicly available website discovered hostnames that describe publicly accessible agency websites, to the extent consistent with the security of Federal information systems but with the presumption of disclosure;

(E) the Director may publish on a publicly available website any analysis conducted and data collected relating to compliance with Federal mandates and industry best practices, to the extent consistent with the security of Federal information systems but with the presumption of disclosure; and

(F) the Director shall—

(i) collect information on the use of non-.gov internet domain suffixes by agencies for their official online services;

(ii) collect information on the use of non-.gov internet domain suffixes by State, local, Tribal, and territorial governments; and

(iii) publish the information collected under clause (i) on a publicly available website to the extent consistent with the security of the Federal information systems, but with the presumption of disclosure.

(3) NATIONAL SECURITY COORDINATION.—

(A) IN GENERAL.—In carrying out this subsection, the Director shall inventory, collect, and publish hostnames and services in a manner consistent with the protection of national security information.

(B) LIMITATION.—The Director may not inventory, collect, or publish hostnames or services under this subsection if the Director, in coordination with other heads of

agencies, as appropriate, determines that the collection or publication would—

(i) disrupt a law enforcement investigation;

(ii) endanger national security or intelligence activities;

(iii) impede national defense activities or military operations; or

(iv) hamper security remediation actions.

(4) STRATEGY.—Not later than 180 days after the date of enactment of this section, the Director shall develop and submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on House Administration of the House of Representatives a strategy to utilize the information collected under this subsection for countering malicious cyber activity.

SEC. [2215] *2216*. JOINT CYBER PLANNING OFFICE.

(a) ESTABLISHMENT OF OFFICE.—There is established in the Agency an office for joint cyber planning (in this section referred to as the "Office") to develop, for public and private sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to protect, detect, respond to, and recover from cybersecurity risks or incidents or limit, mitigate, or defend against coordinated, malicious cyber operations that pose a potential risk to critical infrastructure or national interests. The Office shall be headed by a senior official of the Agency selected by the Director.

(b) PLANNING AND EXECUTION.—In leading the development of plans for cyber defense operations pursuant to subsection (a), the head of the Office shall—

(1) coordinate with relevant Federal departments and agencies to establish processes and procedures necessary to develop and maintain ongoing coordinated plans for cyber defense operations;

(2) leverage cyber capabilities and authorities of participating Federal departments and agencies, as appropriate, in furtherance of plans for cyber defense operations;

(3) ensure that plans for cyber defense operations are, to the greatest extent practicable, developed in collaboration with relevant private sector entities, particularly in areas in which such entities have comparative advantages in limiting, mitigating, or defending against a cybersecurity risk or incident or coordinated, malicious cyber operation;

(4) ensure that plans for cyber defense operations, as appropriate, are responsive to potential adversary activity conducted in response to United States offensive cyber operations;

(5) facilitate the exercise of plans for cyber defense operations, including by developing and modeling scenarios based on an understanding of adversary threats to, vulnerability of, and potential consequences of disruption or compromise of critical infrastructure;

(6) coordinate with and, as necessary, support relevant Federal departments and agencies in the establishment of procedures, development of additional plans, including for offensive

and intelligence activities in support of cyber defense operations, and creation of agreements necessary for the rapid execution of plans for cyber defense operations when a cybersecurity risk or incident or malicious cyber operation has been identified; and

(7) support public and private sector entities, as appropriate, in the execution of plans developed pursuant to this section.

(c) COMPOSITION.—The Office shall be composed of—

(1) a central planning staff; and

(2) appropriate representatives of Federal departments and agencies, including—

(A) the Department;

(B) United States Cyber Command;

(C) the National Security Agency;

(D) the Federal Bureau of Investigation;

(E) the Department of Justice; and

(F) the Office of the Director of National Intelligence.

(d) CONSULTATION.—In carrying out its responsibilities described in subsection (b), the Office shall regularly consult with appropriate representatives of non-Federal entities, such as—

(1) State, local, federally-recognized Tribal, and territorial governments;

(2) information sharing and analysis organizations, including information sharing and analysis centers;

(3) owners and operators of critical information systems;

(4) private entities; and

(5) other appropriate representatives or entities, as determined by the Secretary.

(e) INTERAGENCY AGREEMENTS.—The Secretary and the head of a Federal department or agency referred to in subsection (c) may enter into agreements for the purpose of detailing personnel on a reimbursable or non-reimbursable basis.

(f) DEFINITIONS.—In this section:

(1) CYBER DEFENSE OPERATION.—The term "cyber defense operation" means defensive activities performed for a cybersecurity purpose.

(2) CYBERSECURITY PURPOSE.—The term "cybersecurity purpose" has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)).

(3) CYBERSECURITY RISK; INCIDENT.—The terms "cybersecurity risk" and "incident" have the meanings given such terms in section 2209.

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

SEC. [2215] *2217*. CYBERSECURITY STATE COORDINATOR.

(a) APPOINTMENT.—The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(b) DUTIES.—The duties of a Cybersecurity State Coordinator appointed under subsection (a) shall include—

(1) building strategic public and, on a voluntary basis, private sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;

(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;

(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;

(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;

(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity incidents;

(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;

(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;

(9) coordinating with appropriate officials within the Agency; and

(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in the United States and reducing the impact of cyber threats to non-Federal entities.

(c) FEEDBACK.—The Director shall consult with relevant State, local, Tribal, and territorial officials regarding the appointment, and State, local, Tribal, and territorial officials and other non-Federal entities regarding the performance, of the Cybersecurity State Coordinator of a State.

SEC. [2215] *2218*. SECTOR RISK MANAGEMENT AGENCIES.

(a) IN GENERAL.—Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency, in coordination with the Director, shall—

(1) provide specialized sector-specific expertise to critical infrastructure owners and operators within its designated critical infrastructure sector or subsector of such sector; and

(2) support programs and associated activities of such sector or subsector of such sector.

(b) IMPLEMENTATION.—In carrying out this section, Sector Risk Management Agencies shall—

(1) coordinate with the Department and, as appropriate, other relevant Federal departments and agencies;

(2) collaborate with critical infrastructure owners and operators within the designated critical infrastructure sector or subsector of such sector; and

(3) coordinate with independent regulatory agencies, and State, local, Tribal, and territorial entities, as appropriate.

(c) RESPONSIBILITIES.—Consistent with applicable law, Presidential directives, Federal regulations, and strategic guidance from the Secretary, each Sector Risk Management Agency shall utilize its specialized expertise regarding its designated critical infrastructure sector or subsector of such sector and authorities under applicable law to—

(1) support sector risk management, in coordination with the Director, including—

(A) establishing and carrying out programs to assist critical infrastructure owners and operators within the designated sector or subsector of such sector in identifying, understanding, and mitigating threats, vulnerabilities, and risks to their systems or assets, or within a region, sector, or subsector of such sector; and

(B) recommending security measures to mitigate the consequences of destruction, compromise, and disruption of systems and assets;

(2) assess sector risk, in coordination with the Director, including—

(A) identifying, assessing, and prioritizing risks within the designated sector or subsector of such sector, considering physical security and cybersecurity threats, vulnerabilities, and consequences; and

(B) supporting national risk assessment efforts led by the Department;

(3) sector coordination, including—

(A) serving as a day-to-day Federal interface for the prioritization and coordination of sector-specific activities and responsibilities under this title;

(B) serving as the Federal Government coordinating council chair for the designated sector or subsector of such sector; and

(C) participating in cross-sector coordinating councils, as appropriate;

(4) facilitating, in coordination with the Director, the sharing with the Department and other appropriate Federal department of information regarding physical security and cybersecurity threats within the designated sector or subsector of such sector, including—

(A) facilitating, in coordination with the Director, access to, and exchange of, information and intelligence necessary to strengthen the security of critical infrastructure, including through information sharing and analysis organizations and the national cybersecurity and communications integration center established pursuant to section 2209;

(B) facilitating the identification of intelligence needs and priorities of critical infrastructure owners and operators in the designated sector or subsector of such sector, in coordination with the Director of National Intelligence and the heads of other Federal departments and agencies, as appropriate;

(C) providing the Director, and facilitating awareness within the designated sector or subsector of such sector, of

ongoing, and where possible, real-time awareness of identified threats, vulnerabilities, mitigations, and other actions related to the security of such sector or subsector of such sector; and

(D) supporting the reporting requirements of the Department under applicable law by providing, on an annual basis, sector-specific critical infrastructure information;

(5) supporting incident management, including—

(A) supporting, in coordination with the Director, incident management and restoration efforts during or following a security incident; and

(B) supporting the Director, upon request, in national cybersecurity asset response activities for critical infrastructure; and

(6) contributing to emergency preparedness efforts, including—

(A) coordinating with critical infrastructure owners and operators within the designated sector or subsector of such sector and the Director in the development of planning documents for coordinated action in the event of a natural disaster, act of terrorism, or other man-made disaster or emergency;

(B) participating in and, in coordination with the Director, conducting or facilitating, exercises and simulations of potential natural disasters, acts of terrorism, or other man-made disasters or emergencies within the designated sector or subsector of such sector; and

(C) supporting the Department and other Federal departments or agencies in developing planning documents or conducting exercises or simulations when relevant to the designated sector or subsector or such sector.

SEC. [2216] *2219*. CYBERSECURITY ADVISORY COMMITTEE.

(a) ESTABLISHMENT.—The Secretary shall establish within the Agency a Cybersecurity Advisory Committee (referred to in this section as the "Advisory Committee").

(b) DUTIES.—

(1) IN GENERAL.—The Advisory Committee shall advise, consult with, report to, and make recommendations to the Director, as appropriate, on the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

(2) RECOMMENDATIONS.—

(A) IN GENERAL.—The Advisory Committee shall develop, at the request of the Director, recommendations for improvements to advance the cybersecurity mission of the Agency and strengthen the cybersecurity of the United States.

(B) RECOMMENDATIONS OF SUBCOMMITTEES.—Recommendations agreed upon by subcommittees established under subsection (d) for any year shall be approved by the Advisory Committee before the Advisory Committee submits to the Director the annual report under paragraph (4) for that year.

(3) PERIODIC REPORTS.—The Advisory Committee shall periodically submit to the Director—

(A) reports on matters identified by the Director; and

(B) reports on other matters identified by a majority of the members of the Advisory Committee.

(4) ANNUAL REPORT.—

(A) IN GENERAL.—The Advisory Committee shall submit to the Director an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year.

(B) PUBLICATION.—Not later than 180 days after the date on which the Director receives an annual report for a year under subparagraph (A), the Director shall publish a public version of the report describing the activities of the Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5, United States Code.

(5) FEEDBACK.—Not later than 90 days after receiving any recommendation submitted by the Advisory Committee under paragraph (2), (3), or (4), the Director shall respond in writing to the Advisory Committee with feedback on the recommendation. Such a response shall include—

(A) with respect to any recommendation with which the Director concurs, an action plan to implement the recommendation; and

(B) with respect to any recommendation with which the Director does not concur, a justification for why the Director does not plan to implement the recommendation.

(6) CONGRESSIONAL NOTIFICATION.—Not less frequently than once per year after the date of enactment of this section, the Director shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives a briefing on feedback from the Advisory Committee.

(7) GOVERNANCE RULES.—The Director shall establish rules for the structure and governance of the Advisory Committee and all subcommittees established under subsection (d).

(c) MEMBERSHIP.—

(1) APPOINTMENT.—

(A) IN GENERAL.—Not later than 180 days after the date of enactment of the Cybersecurity Advisory Committee Authorization Act of 2020, the Director shall appoint the members of the Advisory Committee.

(B) COMPOSITION.—The membership of the Advisory Committee shall consist of not more than 35 individuals.

(C) REPRESENTATION.—

(i) IN GENERAL.—The membership of the Advisory Committee shall satisfy the following criteria:

(I) Consist of subject matter experts.

(II) Be geographically balanced.

(III) Include representatives of State, local, and Tribal governments and of a broad range of industries, which may include the following:

(aa) Defense.

(bb) Education.
(cc) Financial services and insurance.
(dd) Healthcare.
(ee) Manufacturing.
(ff) Media and entertainment.
(gg) Chemicals.
(hh) Retail.
(ii) Transportation.
(jj) Energy.
(kk) Information Technology.
(ll) Communications.
(mm) Other relevant fields identified by the Director.

(ii) PROHIBITION.—Not fewer than one member nor more than three members may represent any one category under clause (i)(III).

(iii) PUBLICATION OF MEMBERSHIP LIST.—The Advisory Committee shall publish its membership list on a publicly available website not less than once per fiscal year and shall update the membership list as changes occur.

(2) TERM OF OFFICE.—

(A) TERMS.—The term of each member of the Advisory Committee shall be two years, except that a member may continue to serve until a successor is appointed.

(B) REMOVAL.—The Director may review the participation of a member of the Advisory Committee and remove such member any time at the discretion of the Director.

(C) REAPPOINTMENT.—A member of the Advisory Committee may be reappointed for an unlimited number of terms.

(3) PROHIBITION ON COMPENSATION.—The members of the Advisory Committee may not receive pay or benefits from the United States Government by reason of their service on the Advisory Committee.

(4) MEETINGS.—

(A) IN GENERAL.—The Director shall require the Advisory Committee to meet not less frequently than semiannually, and may convene additional meetings as necessary.

(B) PUBLIC MEETINGS.—At least one of the meetings referred to in subparagraph (A) shall be open to the public.

(C) ATTENDANCE.—The Advisory Committee shall maintain a record of the persons present at each meeting.

(5) MEMBER ACCESS TO CLASSIFIED INFORMATION.—

(A) IN GENERAL.—Not later than 60 days after the date on which a member is first appointed to the Advisory Committee and before the member is granted access to any classified information, the Director shall determine, for the purposes of the Advisory Committee, if the member should be restricted from reviewing, discussing, or possessing classified information.

(B) ACCESS.—Access to classified materials shall be managed in accordance with Executive Order No. 13526 of De-

cember 29, 2009 (75 Fed. Reg. 707), or any subsequent corresponding Executive Order.

(C) PROTECTIONS.—A member of the Advisory Committee shall protect all classified information in accordance with the applicable requirements for the particular level of classification of such information.

(D) RULE OF CONSTRUCTION.—Nothing in this paragraph shall be construed to affect the security clearance of a member of the Advisory Committee or the authority of a Federal agency to provide a member of the Advisory Committee access to classified information.

(6) CHAIRPERSON.—The Advisory Committee shall select, from among the members of the Advisory Committee—

(A) a member to serve as chairperson of the Advisory Committee; and

(B) a member to serve as chairperson of each subcommittee of the Advisory Committee established under subsection (d).

(d) SUBCOMMITTEES.—

(1) IN GENERAL.—The Director shall establish subcommittees within the Advisory Committee to address cybersecurity issues, which may include the following:

(A) Information exchange.

(B) Critical infrastructure.

(C) Risk management.

(D) Public and private partnerships.

(2) MEETINGS AND REPORTING.—Each subcommittee shall meet not less frequently than semiannually, and submit to the Advisory Committee for inclusion in the annual report required under subsection (b)(4) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

(3) SUBJECT MATTER EXPERTS.—The chair of the Advisory Committee shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee.

SEC. [2217] *2220*. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.

(a) ESTABLISHMENT.—

(1) IN GENERAL.—The Cybersecurity Education and Training Assistance Program (referred to in this section as "CETAP") is established within the Agency.

(2) PURPOSE.—The purpose of CETAP shall be to support the effort of the Agency in building and strengthening a national cybersecurity workforce pipeline capacity through enabling elementary and secondary cybersecurity education, including by—

(A) providing foundational cybersecurity awareness and literacy;

(B) encouraging cybersecurity career exploration; and

(C) supporting the teaching of cybersecurity skills at the elementary and secondary education levels.

(b) REQUIREMENTS.—In carrying out CETAP, the Director shall—

(1) ensure that the program—

(A) creates and disseminates cybersecurity-focused curricula and career awareness materials appropriate for use at the elementary and secondary education levels;

(B) conducts professional development sessions for teachers;

(C) develops resources for the teaching of cybersecurity-focused curricula described in subparagraph (A);

(D) provides direct student engagement opportunities through camps and other programming;

(E) engages with State educational agencies and local educational agencies to promote awareness of the program and ensure that offerings align with State and local curricula;

(F) integrates with existing post-secondary education and workforce development programs at the Department;

(G) promotes and supports national standards for elementary and secondary cyber education;

(H) partners with cybersecurity and education stakeholder groups to expand outreach; and

(I) any other activity the Director determines necessary to meet the purpose described in subsection (a)(2); and

(2) enable the deployment of CETAP nationwide, with special consideration for underserved populations or communities.

(c) BRIEFINGS.—

(1) IN GENERAL.—Not later than 1 year after the establishment of CETAP, and annually thereafter, the Secretary shall brief the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives on the program.

(2) CONTENTS.—Each briefing conducted under paragraph (1) shall include—

(A) estimated figures on the number of students reached and teachers engaged;

(B) information on outreach and engagement efforts, including the activities described in subsection (b)(1)(E);

(C) information on new curricula offerings and teacher training platforms; and

(D) information on coordination with post-secondary education and workforce development programs at the Department.

(d) MISSION PROMOTION.—The Director may use appropriated amounts to purchase promotional and recognition items and marketing and advertising services to publicize and promote the mission and services of the Agency, support the activities of the Agency, and to recruit and retain Agency personnel.

SEC. 2220A. STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

(a) DEFINITIONS.—In this section:

(1) CYBER THREAT INDICATOR.—The term "cyber threat indicator" has the meaning given the term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501).

(2) CYBERSECURITY PLAN.—The term "Cybersecurity Plan" means a plan submitted by an eligible entity under subsection (e)(1).

(3) ELIGIBLE ENTITY.—The term "eligible entity" means—

(A) a State; or

(B) an Indian tribe that, 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—

(i) notifies the Secretary that the Indian tribe intends to develop a Cybersecurity Plan; and

(ii) agrees to forfeit any distribution under subsection (n)(2).

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

(5) INDIAN TRIBE; TRIBAL ORGANIZATION.—The term "Indian tribe" or "Tribal organization" has the meaning given that term in section 4(e) of the of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304(e)).

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

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

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

(9) RANSOMWARE INCIDENT.—The term "ransomware incident" means an incident that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system for the purpose of coercing the information system's owner, operator, or another person.

(10) STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.—The term "State and Local Cybersecurity Grant Program" means the program established under subsection (b).

(11) STATE AND LOCAL CYBERSECURITY RESILIENCE COMMITTEE.—The term "State and Local Cybersecurity Resilience Committee" means the committee established under subsection (o)(1).

(b) ESTABLISHMENT.—

(1) IN GENERAL.—The Secretary, acting through the Director, shall establish a program, to be known as the "the State and Local Cybersecurity Grant Program", to award grants to eligible entities to address cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations.

(2) APPLICATION.—An eligible entity seeking a grant under the State and Local Cybersecurity Grant Program shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(c) BASELINE REQUIREMENTS.—An eligible entity or multistate group that receives a grant under this section shall use the grant in compliance with—

(1)(A) the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group; and

(B) the Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments developed under section 2210(e)(1); or

(2) activities carried out under paragraphs (3), (4), and (5) of subsection (h).

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

(e) CYBERSECURITY PLANS.—

(1) IN GENERAL.—An eligible entity applying for a grant under this section shall submit to the Secretary a Cybersecurity Plan for approval.

(2) REQUIRED ELEMENTS.—A Cybersecurity Plan of an eligible entity shall—

(A) incorporate, to the extent practicable, any existing plans of the eligible entity to protect against cybersecurity risks and cybersecurity threats to information systems of State, local, or Tribal organizations;

(B) describe, to the extent practicable, how the eligible entity will—

(i) manage, monitor, and track information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and the information technology deployed on those information systems, including legacy information systems and information technology that are no longer supported by the manufacturer of the systems or technology;

(ii) monitor, audit, and track activity between information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity and between those information systems and information systems not owned or operated by the eligible entity or by local or Tribal organizations within the jurisdiction of the eligible entity;

(iii) enhance the preparation, response, and resilience of information systems, applications, and user accounts owned or operated by or on behalf of the eligible entity or local or Tribal organizations against cybersecurity risks and cybersecurity threats;

(iv) implement a process of continuous cybersecurity vulnerability assessments and threat mitigation practices prioritized by degree of risk to address cybersecurity risks and cybersecurity threats on information systems of the eligible entity or local or Tribal organizations;

(v) ensure that State, local, and Tribal organizations that own or operate information systems that are located within the jurisdiction of the eligible entity—

(I) adopt best practices and methodologies to enhance cybersecurity, such as the practices set forth in the cybersecurity framework developed by, and the cyber supply chain risk management best prac-

tices identified by, the National Institute of Standards and Technology; and

(II) utilize knowledge bases of adversary tools and tactics to assess risk;

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

(vii) ensure continuity of operations of the eligible entity and local, and Tribal organizations in the event of a cybersecurity incident (including a ransomware incident), including by conducting exercises to practice responding to such an incident;

(viii) use the National Initiative for Cybersecurity Education Cybersecurity Workforce Framework developed by the National Institute of Standards and Technology to identify and mitigate any gaps in the cybersecurity workforces of State, local, or Tribal organizations, enhance recruitment and retention efforts for such workforces, and bolster the knowledge, skills, and abilities of State, local, and Tribal organization personnel to address cybersecurity risks and cybersecurity threats, such as through cybersecurity hygiene training;

(ix) ensure continuity of communications and data networks within the jurisdiction of the eligible entity between the eligible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity in the event of an incident involving such communications or data networks within the jurisdiction of the eligible entity;

(x) 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 the jurisdiction of the eligible entity;

(xi) enhance capabilities to share cyber threat indicators and related information between the eligible entity and local and Tribal organizations that own or operate information systems within the jurisdiction of the eligible entity, including by expanding existing information sharing agreements with the Department;

(xii) enhance the capability of the eligible entity to share cyber threat indictors and related information with the Department;

(xiii) leverage cybersecurity services offered by the Department;

(xiv) develop and coordinate strategies to address cybersecurity risks and cybersecurity threats to information systems of the eligible entity in consultation with—

(I) local and Tribal organizations within the jurisdiction of the eligible entity; and

(II) as applicable—

(aa) States that neighbor the jurisdiction of the eligible entity or, as appropriate, members

of an information sharing and analysis organization; and

(bb) countries that neighbor the jurisdiction of the eligible entity; and

(xv) implement an information technology and operational technology modernization cybersecurity review process that ensures alignment between information technology and operational technology cybersecurity objectives;

(C) describe, to the extent practicable, the individual responsibilities of the eligible entity and local and Tribal organizations within the jurisdiction of the eligible entity in implementing the plan;

(D) outline, to the extent practicable, the necessary resources and a timeline for implementing the plan; and

(E) describe how the eligible entity will measure progress towards implementing the plan.

(3) DISCRETIONARY ELEMENTS.—A Cybersecurity Plan of an eligible entity may include a description of—

(A) cooperative programs developed by groups of local and Tribal organizations within the jurisdiction of the eligible entity to address cybersecurity risks and cybersecurity threats; and

(B) programs provided by the eligible entity to support local and Tribal organizations and owners and operators of critical infrastructure to address cybersecurity risks and cybersecurity threats.

(4) MANAGEMENT OF FUNDS.—An eligible entity applying for a grant under this section shall agree to designate the Chief Information Officer, the Chief Information Security Officer, or an equivalent official of the eligible entity as the primary official for the management and allocation of funds awarded under this section.

(f) MULTISTATE GRANTS.—

(1) IN GENERAL.—The Secretary, acting through the Director, may award grants under this section to a group of two or more eligible entities to support multistate efforts to address cybersecurity risks and cybersecurity threats to information systems within the jurisdictions of the eligible entities.

(2) SATISFACTION OF OTHER REQUIREMENTS.—In order to be eligible for a multistate grant under this subsection, each eligible entity that comprises a multistate group shall submit to the Secretary—

(A) a Cybersecurity Plan for approval in accordance with subsection (i); and

(B) a plan for establishing a cybersecurity planning committee under subsection (g).

(3) APPLICATION.—

(A) IN GENERAL.—A multistate group applying for a multistate grant under paragraph (1) shall submit to the Secretary an application at such time, in such manner, and containing such information as the Secretary may require.

(B) MULTISTATE PROJECT DESCRIPTION.—An application of a multistate group under subparagraph (A) shall include a plan describing—

(i) the division of responsibilities among the eligible entities that comprise the multistate group for administering the grant for which application is being made;

(ii) the distribution of funding from such a grant among the eligible entities that comprise the multistate group; and

(iii) how the eligible entities that comprise the multistate group will work together to implement the Cybersecurity Plan of each of those eligible entities.

(g) PLANNING COMMITTEES.—

(1) IN GENERAL.—An eligible entity that receives a grant under this section shall establish a cybersecurity planning committee to—

(A) assist in the development, implementation, and revision of the Cybersecurity Plan of the eligible entity;

(B) approve the Cybersecurity Plan of the eligible entity; and

(C) assist in the determination of effective funding priorities for a grant under this section in accordance with subsection (h).

(2) COMPOSITION.—A committee of an eligible entity established under paragraph (1) shall—

(A) be comprised of representatives from the eligible entity and counties, cities, towns, Tribes, and public educational and health institutions within the jurisdiction of the eligible entity; and

(B) include, as appropriate, representatives of rural, suburban, and high-population jurisdictions.

(3) CYBERSECURITY EXPERTISE.—Not less than ½ of the representatives of a committee established under paragraph (1) shall have professional experience relating to cybersecurity or information technology.

(4) RULE OF CONSTRUCTION REGARDING EXISTING PLANNING COMMITTEES.—Nothing in this subsection may be construed to require an eligible entity to establish a cybersecurity planning committee if the eligible entity has established and uses a multijurisdictional planning committee or commission that meets, or may be leveraged to meet, the requirements of this subsection.

(h) USE OF FUNDS.—An eligible entity that receives a grant under this section shall use the grant to—

(1) implement the Cybersecurity Plan of the eligible entity;

(2) develop or revise the Cybersecurity Plan of the eligible entity; or

(3) assist with activities that address imminent cybersecurity risks or cybersecurity threats to the information systems of the eligible entity or a local or Tribal organization within the jurisdiction of the eligible entity.

(i) APPROVAL OF PLANS.—

(1) APPROVAL AS CONDITION OF GRANT.—Before an eligible entity may receive a grant under this section, the Secretary, acting through the Director, shall review the Cybersecurity Plan, or any revisions thereto, of the eligible entity and approve such plan, or revised plan, if it satisfies the requirements specified in paragraph (2).

(2) PLAN REQUIREMENTS.—In approving a Cybersecurity Plan of an eligible entity under this subsection, the Director shall ensure that the Cybersecurity Plan—

(A) satisfies the requirements of subsection (e)(2);

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

(C) has been approved by the cybersecurity planning committee of the eligible entity established under subsection (g).

(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 subsection (e) and paragraph (1) of this subsection, the Secretary may award a grant under this section to an eligible entity that does not submit a Cybersecurity Plan to the Secretary if—

(A) the eligible entity certifies to the Secretary that—

(i) the activities that will be supported by the grant are integral to the development of the Cybersecurity Plan of the eligible entity; and

(ii) the eligible entity will submit by September 30, 2023, to the Secretary a Cybersecurity Plan for review, and if appropriate, approval; or

(B) the eligible entity certifies to the Secretary, and the Director confirms, that the eligible entity will use funds from the grant to assist with the activities described in subsection (h)(3).

(j) LIMITATIONS ON USES OF FUNDS.—

(1) IN GENERAL.—An eligible entity that receives a grant under this section may not use the grant—

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

(B) for any recipient cost-sharing contribution;

(C) to pay a demand for ransom in an attempt to—

(i) regain access to information or an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity; or

(ii) prevent the disclosure of information that has been removed without authorization from an information system of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity;

(D) for recreational or social purposes; or

(E) for any purpose that does not address cybersecurity risks or cybersecurity threats on information systems of the eligible entity or of a local or Tribal organization within the jurisdiction of the eligible entity.

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

(3) RULE OF CONSTRUCTION.—Nothing in paragraph (1) may be construed to prohibit the use of grant funds provided to a State, local, or Tribal organization for otherwise permissible

uses under this section on the basis that a State, local, or Tribal organization has previously used State, local, or Tribal funds to support the same or similar uses.

(k) 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.

(l) APPORTIONMENT.—For fiscal year 2022 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, the U.S. 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 eligible entity, bears to

(B) the population of all eligible entities.

(3) MINIMUM ALLOCATION TO INDIAN TRIBES.—

(A) IN GENERAL.—In apportioning amounts under this section, the Secretary shall ensure that, for each fiscal year, directly eligible Tribes collectively receive, from amounts appropriated under the State and Local Cybersecurity Grant Program, not less than an amount equal to three percent of the total amount appropriated for grants under this section.

(B) ALLOCATION.—Of the amount reserved under subparagraph (A), funds shall be allocated in a manner determined by the Secretary in consultation with Indian tribes.

(C) EXCEPTION.—This paragraph shall not apply in any fiscal year in which the Secretary—

(i) receives fewer than five applications from Indian tribes; or

(ii) does not approve at least two application from Indian tribes.

(m) FEDERAL SHARE.—

(1) IN GENERAL.—The Federal share of the cost of an activity carried out using funds made available with a grant under this section may not exceed—

(A) in the case of a grant to an eligible entity—

(i) for fiscal year 2022, 90 percent;

(ii) for fiscal year 2023, 80 percent;

(iii) for fiscal year 2024, 70 percent;

(iv) for fiscal year 2025, 60 percent; and

(v) for fiscal year 2026 and each subsequent fiscal year, 50 percent; and

(B) in the case of a grant to a multistate group—

(i) for fiscal year 2022, 95 percent;

(ii) for fiscal year 2023, 85 percent;

(iii) for fiscal year 2024, 75 percent;

(iv) for fiscal year 2025, 65 percent; and

(v) for fiscal year 2026 and each subsequent fiscal year, 55 percent.

(2) WAIVER.—The Secretary may waive or modify the requirements of paragraph (1) for an Indian tribe if the Secretary determines such a waiver is in the public interest.

(n) RESPONSIBILITIES OF GRANTEES.—

(1) CERTIFICATION.—Each eligible entity or multistate group that receives a grant under this section shall certify to the Secretary that the grant will be used—

(A) for the purpose for which the grant is awarded; and

(B) in compliance with, as the case may be—

(i) the Cybersecurity Plan of the eligible entity;

(ii) the Cybersecurity Plans of the eligible entities that comprise the multistate group; or

(iii) a purpose approved by the Secretary under subsection (h) or pursuant to an exception under subsection (i).

(2) AVAILABILITY OF FUNDS TO LOCAL AND TRIBAL ORGANIZATIONS.—Not later than 45 days after the date on which an eligible entity or multistate group receives a grant under this section, the eligible entity or multistate group shall, without imposing unreasonable or unduly burdensome requirements as a condition of receipt, obligate or otherwise make available to local and Tribal organizations within the jurisdiction of the eligible entity or the eligible entities that comprise the multistate group, and as applicable, consistent with the Cybersecurity Plan of the eligible entity or the Cybersecurity Plans of the eligible entities that comprise the multistate group—

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

(B) with the consent of the local and Tribal organizations, 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 and Tribal organizations, 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 AND TRIBAL ORGANIZATIONS.—An eligible entity or multistate group shall certify to the Secretary that the eligible entity or multistate group has made the distribution to local, Tribal, and territorial governments required under paragraph (2).

(4) EXTENSION OF PERIOD.—

(A) IN GENERAL.—An eligible entity or multistate group may request in writing that the Secretary extend the period of time specified in paragraph (2) for an additional period of time.

(B) APPROVAL.—The Secretary may approve a request for an extension under subparagraph (A) if the Secretary determines the extension is necessary to ensure that the obligation and expenditure of grant funds align with the purpose of the State and Local Cybersecurity 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, the Virgin Islands, or an Indian tribe.

(6) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local or Tribal organization required in accordance with paragraph (2), the local or Tribal organization may petition the Secretary to request that grant funds be provided directly to the local or Tribal organization.

(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 an eligible entity or distribute grant funds previously awarded to such eligible entity directly to the appropriate local or Tribal organization as a replacement grant in an amount the Secretary determines appropriate if such eligible entity violates a requirement of this subsection.

(o) ADVISORY COMMITTEE.—

(1) ESTABLISHMENT.—Not later than 120 days after the date of enactment of this section, the Director shall establish a State and Local Cybersecurity Resilience Committee to provide State, local, and Tribal 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, or Tribal organizations; and

(B) improve the ability of State, local, and Tribal organizations to prevent, protect against, respond to, mitigate, and recover from such cybersecurity risks and cybersecurity threats.

(2) DUTIES.—The committee established under paragraph (1) 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 those plans prior to the approval of the plans under subsection (i);

(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;

(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, or Tribal organizations; and

(ii) improve the cybersecurity resilience of State, local, or Tribal organizations; and

(E) regularly coordinate with the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

(3) MEMBERSHIP.—

(A) NUMBER AND APPOINTMENT.—The State and Local Cybersecurity Resilience Committee established pursuant to paragraph (1) 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) One individual 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) One individual recommended to the Director by the National Congress of American Indians.

(viii) Four individuals who have educational and professional experience relating to cybersecurity work or cybersecurity policy.

(B) TERMS.—

(i) IN GENERAL.—Subject to clause (ii), each member of the State and Local Cybersecurity Resilience Committee shall be appointed for a term of two years.

(ii) REQUIREMENT.—At least two members of the State and Local Cybersecurity Resilience Committee shall also be members of the State, Local, Tribal and Territorial Government Coordinating Council, within the Critical Infrastructure Partnership Advisory Council, established under section 871.

(iii) EXCEPTION.—A term of a member of the State and Local Cybersecurity Resilience Committee shall be three years if the member is appointed initially to the Committee upon the establishment of the Committee.

(iv) TERM REMAINDERS.—Any member of the State and Local Cybersecurity Resilience Committee 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.

(v) VACANCIES.—A vacancy in the State and Local Cybersecurity Resilience Committee shall be filled in the manner in which the original appointment was made.

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

(4) CHAIRPERSON; VICE CHAIRPERSON.—The members of the State and Local Cybersecurity Resilience Committee shall select

a chairperson and vice chairperson from among members of the committee.

(5) PERMANENT AUTHORITY.—Notwithstanding section 14 of the Federal Advisory Committee Act (5 U.S.C. App.), the State and Local Cybersecurity Resilience Committee shall be a permanent authority.

(p) REPORTS.—

(1) ANNUAL REPORTS BY GRANT RECIPIENTS.—

(A) IN GENERAL.—Not later than one year after an eligible entity or multistate group receives funds under this section, the eligible entity or multistate group shall submit to the Secretary a report on the progress of the eligible entity or multistate group in implementing the Cybersecurity Plan of the eligible entity or Cybersecurity Plans of the eligible entities that comprise the multistate group, as the case may be.

(B) ABSENCE OF PLAN.—Not later than 180 days after an eligible entity that does not have a Cybersecurity Plan receives funds under this section for developing its Cybersecurity Plan, the eligible entity shall submit to the Secretary a report describing how the eligible entity obligated and expended grant funds during the fiscal year to—

(i) so develop such a Cybersecurity Plan; or

(ii) assist with the activities described in subsection (h)(3).

(2) ANNUAL REPORTS TO CONGRESS.—Not less frequently than once per 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 date on which the strategy is issued under section 2210.

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

(C) Reducing cybersecurity risks and cybersecurity threats to information systems, applications, and user accounts owned or operated by or on behalf of State, local, and Tribal organizations as a result of the award of such grants.

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

(1) for each of fiscal years 2022 through 2026, $500,000,000; and

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

SEC. 2220B. CYBERSECURITY RESOURCE GUIDE DEVELOPMENT FOR STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENT OFFICIALS.

The Secretary, acting through the Director, shall develop, regularly update, and maintain 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 (as

such term is defined in section 2209), cybersecurity threats, and incidents (as such term is defined in section 2209).

* * * * * * *

SECTION 904 OF DIVISION U OF THE CONSOLIDATED APPROPRIATIONS ACT, 2021

SEC. 904. DUTIES OF DEPARTMENT OF HOMELAND SECURITY.

(a) PURPOSE.—The purpose of the.gov internet domain program is to—

(1) legitimize and enhance public trust in government entities and their online services;

(2) facilitate trusted electronic communication and connections to and from government entities;

(3) provide simple and secure registration of.gov internet domains;

(4) improve the security of the services hosted within these.gov internet domains, and of the.gov namespace in general; and

(5) enable the discoverability of government services to the public and to domain registrants.

(b) DUTIES AND AUTHORITIES RELATING TO THE.GOV INTERNET DOMAIN.—

(1) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act *of 2002* (6 U.S.C. 651 et seq.) is amended—

(A) (Omitted amendatory)

(B) (Omitted amendatory)

(2) ADDITIONAL DUTIES.—

(A) OUTREACH STRATEGY.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Administrator and entities representing State, local, Tribal, or territorial governments, shall develop and submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Rules and Administration of the Senate and the Committee on Homeland Security, the Committee on Oversight and Reform, and the Committee on House Administration of the House of Representatives an outreach strategy to local, Tribal, and territorial governments and other publicly controlled entities as determined by the Director to inform and support migration to the.gov internet domain, which shall include—

(i) stakeholder engagement plans; and

(ii) information on how migrating information technology systems to the.gov internet domain is beneficial to that entity, including benefits relating to cybersecurity and the supporting services offered by the Federal Government.

(B) REFERENCE GUIDE.—Not later than 1 year after the date of enactment of this Act, the Director, in consultation with the Administrator and entities representing State, local, Tribal, or territorial governments, shall develop and publish on a publicly available website a reference guide

for migrating online services to the.gov internet domain, which shall include—

(i) process and technical information on how to carry out a migration of common categories of online services, such as web and email services;

(ii) best practices for cybersecurity pertaining to registration and operation of a.gov internet domain; and

(iii) an outline of specific security enhancements the.gov program intends to provide to users during that 5-year period.

(3) (Omitted amendatory)

(c) (Omitted amendatory)

* * * * * * *

○