.....

(Original Signature of Member)

119TH CONGRESS
1ST SESSION

H. R. _____

To amend the Homeland Security Act of 2002 to reauthorize the State and local cybersecurity grant program of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. OGLES introduced the following bill; which was referred to the Committee on _____

A BILL

To amend the Homeland Security Act of 2002 to reauthorize the State and local cybersecurity grant program of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Protecting Information by Local Leaders for Agency Resilience Act'' or the ''PILLAR Act''.

SEC. 2. REAUTHORIZATION OF CISA STATE AND LOCAL CYBERSECURITY GRANT PROGRAM.

Section 2220A of the Homeland Security Act of 2002 (6 U.S.C. 665g) is amended—

(1) in subsection (a)—

(A) by redesignating paragraphs (1), (2), (3), (4), (5), (6), and (7) as paragraphs (3), (4), (6), (8), (9), (10), and (11), respectively;

(B) by inserting before paragraph (3), as so redesignated, the following new paragraphs:

''(1) ARTIFICIAL INTELLIGENCE.—The term 'artificial intelligence' has the meaning given such term in section 5002(3) of the National Artificial Intelligence Initiative Act of 2020 (enacted as division E of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (15 U.S.C. 9401(3))).

''(2) ARTIFICIAL INTELLIGENCE SYSTEM.—The term 'artificial intelligence system' means any data system, software, hardware, application tool, or utility that operates in whole or in part using artificial intelligence.'';

(C) by inserting after paragraph (4), as so redesignated, the following new paragraph:

''(5) FOREIGN ENTITY OF CONCERN.—The term 'foreign entity of concern' has the meaning

given such term in section 10634 of the Research and Development, Competition, and Innovation Act (42 U.S.C. 19237; Public Law 117–167; popularly referred to as the 'CHIPS and Science Act').''; and

(D) by inserting after paragraph (6), as so redesignated, the following new paragraph:

''(7) MULTI-FACTOR AUTHENTICATION.—The term 'multi factor authentication' means an authentication system that requires more than one distinct type of authentication factor for successful authentication of a user, including by using a multi-factor authenticator or by combining single-factor authenticators that provide different types of factors.'';

(2) in subsection (b)(1), by striking ''information systems owned'' and inserting ''information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or'';

(3) in subsection (d)(4), by striking ''to the information systems owned'' and inserting ''to the information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or''; and

(4) in subsection (e)—

(A) in paragraph (2)—

(i) in subparagraph (A)(i), by striking ''information systems owned'' and inserting ''information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or'';

(ii) in subparagraph (B)—

(I) by amending clauses (i) through (v) to read as follows:

''(i) manage, monitor, and track applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, that are maintained, owned, or operated by, or on behalf of, the eligible entity, or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, and the information technology deployed on such information systems or operational technology systems (as the case may be), including legacy information systems, operational technology systems, and information technology that are no longer sup-

ported by the manufacturer of the systems or technology at issue;

''(ii) monitor, audit, and track network traffic and activity transiting or traveling to or from applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

''(iii) enhance the preparation, response, and resiliency of applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, 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 applications, user accounts, and information systems and operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity;

''(v) ensure that the eligible entity and, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity, adopt and use best practices and methodologies to enhance cybersecurity, particularly identity and access management solutions such as multi-factor authentication, which may include—

''(I) the practices set forth in a cybersecurity framework developed by the National Institute of Standards and Technology or the Agency;

''(II) cyber chain supply chain risk management best practices identified by the National Institute of Standards and Technology or the Agency;

''(III) knowledge bases of adversary tools and tactics;

''(IV) technologies such as artificial intelligence; and

''(V) improving cyber incident response capabilities through adoption of automated cybersecurity practices;'';

(II) in clause (x), by inserting ''or operational technology systems, including either or both of such systems using artificial intelligence,'' after ''information systems'';

(III) in clause (xi)(I), by inserting '', including through Department of Homeland Security State, Local, and Regional Fusion Center Initiative under section 210(A)'' before the semicolon; and

(IV) in clause (xii), by inserting ‘‘, including for bolstering the resilience of outdated or vulnerable information systems or operational technology systems, including either or both of such systems using artificial intelligence’’ before the semicolon;

(V) by amending clause (xiii) to read as follows:

‘‘(xiii) implement an information technology or operational technology, including either or both of such systems using artificial intelligence, modernization cybersecurity review process that ensures alignment between information technology, operational technology, and artificial intelligence cybersecurity objectives;’’;

(VI) in clause (xiv)(II)—

(aa) in item (aa), by striking ‘‘and’’ after the semicolon;

(bb) in item (bb), by inserting ‘‘and’’ after the semicolon; and

(cc) by adding at the end the following new item:

''(cc) academic and nonprofit entities, including cybersecurity clinics and other nonprofit technical assistance programs;''; and

(VII) by amending clause (xv) to read as follows:

''(xv) ensure adequate access to, and participation in, the services and programs described in this subparagraph by rural areas and other local governments with small populations within the jurisdiction of the eligible entity, including by direct outreach to such rural areas and local governments with small populations; and''; and

(iii) in subparagraph (F)—

(I) in clause (i), by striking ''and'' after the semicolon;

(II) by amending clause (ii) to read as follows:

''(ii) reducing cybersecurity risks to, and identifying, responding to, and recovering from cybersecurity threats to, information systems or operational technology systems, including either or both of such

systems using artificial intelligence, maintained, owned or operated by, or on behalf of, the eligible entity or, if the eligible entity is a State, local governments within the jurisdiction of the eligible entity; and''; and

(III) by adding at the end the following new clause:

''(iii) assuming the cost or partial cost of cybersecurity investments made as a result of the plan.''; and

(B) in paragraph (3)(A), by striking ''the Multi-State Information Sharing and Analysis Center'' and inserting ''Information Sharing and Analysis Organizations'';

(5) in subsection (g)—

(A) in paragraph (2)(A)(ii), by inserting ''including, as appropriate, representatives of rural, suburban, and high-population jurisdictions (including such jurisdictions with low or otherwise limited operating budgets)'' before the semicolon; and

(B) by amending paragraph (5) to read as follows:

''(5) RULE OF CONSTRUCTION REGARDING CONTROL OF CERTAIN INFORMATION SYSTEMS OR OPER-

ATIONAL TECHNOLOGY SYSTEMS OF ELIGIBLE ENTITIES.—Nothing in this subsection may be construed to permit a cybersecurity planning committee of an eligible entity that meets the requirements of this subsection to make decisions relating to information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned, or operated by, or on behalf of, the eligible entity.'';

(6) in subsection (i)—

(A) in paragraph (1)(B), by striking ''2-year period'' and inserting ''3-year period'';

(B) in paragraph (3)—

(i) in the matter preceding subparagraph (A), by striking ''2023'' and inserting ''2027''; and

(ii) in subparagraph (B), by striking ''2023'' and inserting ''2027''; and

(C) in paragraph (4)—

(i) in the matter preceding subparagraph (A), by striking ''shall'' and inserting ''may''; and

(ii) in subparagraph (A), by striking ''information systems owned'' inserting ''information systems or operational tech-

nology systems, including either or both of such systems using artificial intelligence, maintained, owned,'';

(7) in subsection (j)(1)—

(A) in subparagraph (D), by striking ''or'' after the semicolon;

(B) in subparagraph (E)—

(i) by striking ''information systems owned'' and inserting ''information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned,''; and

(ii) by striking the period and inserting a semicolon; and

(C) by adding at the end the following new subparagraphs:

''(E) to purchase software or hardware, or products or services of such software or hardware, as the case may be, that do not align with guidance relevant to such software or hardware, or products or services, as the case may be, provided by the Agency, including Secure by Design or successor guidance; or

''(F) to purchase software or hardware, or products or services of such software or hardware, as the case may be, that are designed, developed, operated, maintained, manufactured, or sold by a foreign entity of concern and do not align with guidance provided by the Agency.'';

(8) in subsection (l), in the matter preceding paragraph (1), by striking ''2022'' and inserting ''2026'';

(9) in subsection (m), by amending paragraph (1) to read as follows:

''(1) IN GENERAL.—The Federal share of activities carried out using funds made available pursuant to the award of a grant under this section may not exceed—

''(A) in the case of a grant to an eligible entity, 60 percent for each fiscal year through fiscal year 2035; and

''(B) in the case of a grant to a multi-entity group, 70 percent for each fiscal year through fiscal year 2035.

Notwithstanding subparagraphs (A) and (B), the Federal share of the cost for an eligible entity or multi-entity group shall be 65 percent for an entity and 75 percent for a multi-group entity for each fis-

cal year beginning with fiscal year 2028 through fiscal year 2035 if such entity or multi-entity group entity, as the case may be, implements or enables, by not later than October 1, 2027, multi-factor authentication and identity and access management tools that support multi-factor authentication with respect to critical infrastructure, including the information systems and operational technology systems, including either or both of such systems using artificial intelligence, of such critical infrastructure, that is within the jurisdiction of such entity or multi-entity group is responsible.'';

(10) in subsection (n)—

(A) in paragraph (2)—

(i) in subparagraph (A)—

(I) in the matter preceding clause (i), by striking ''a grant'' and inserting ''a grant on or after January 1, 2026, or changes the allocation of funding as permissible within the allowances of''; and

(II) by amending clauses (ii) and (iii) to read as follows:

''(ii) with the consent of the local governments, items, in-kind services, capabili-

ties, or activities, or a combination of funding and other services, having a value of not less than 80 percent of the amount of the grant; or

''(iii) with the consent of the local governments, grant funds combined with other items, in-kind services, capabilities, or activities, or a combination of funding and other services, having the total value of not less than 80 percent of the amount of the grant.''; and

(ii) in subparagraph (B), by amending clauses (ii) and (iii) to read as follows:

''(ii) items, in kind services, capabilities, or activities, or a combination of funding and other services, having a value of not less than 25 percent of the amount of the grant awarded to the eligible entity; or

''(iii) grant funds combined with other items, in kind services, capabilities, or activities, or a combination of funding and other services, having the total value of not less than 25 percent of the grant awarded to the eligible entity.''; and

(B) by amending paragraph (5) to read as follows:

''(5) DIRECT FUNDING.—If an eligible entity does not make a distribution to a local government required under paragraph (2) within 60 days of the anticipated grant disbursement date, such local government may petition the Secretary to request the Secretary to provide funds directly to such local government.'';

(11) in subsection (o), in the matter preceding paragraph (1), by inserting ''and representatives from rural areas and other local governments with small populations'' after ''governments'';

(12) by redesignating subsections (p) through (s) as subsections (q) through (t), respectively;

(13) by inserting after subsection (o) the following new subsection:

''(p) OUTREACH TO LOCAL GOVERNMENTS.—The Secretary, acting through the Director, shall implement an outreach plan to inform local governments, including those in rural areas or with small populations, about no-cost cybersecurity service offerings available from the Agency.'';

(14) in subsection (r), as so redesignated—

(A) in paragraph (1)(A)—

(i) in clause (i), by striking ''and'' after the semicolon;

(ii) in clause (ii)—

(I) by striking ''information systems owned'' inserting ''information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned,''; and

(II) by striking the period and inserting ''; and''; and

(iii) by adding at the end the following new clause:

''(iii) assuming the costs associated with continuing the programs specified in the Cybersecurity Plan by including such programs in State and local government budgets upon full expenditure of grant funds by the eligible entity.'';

(B) in paragraph (2)(E)(ii), by striking ''information systems owned'' and inserting ''information systems or operational technology systems, including either or both of such systems using artificial intelligence, maintained, owned''; and

(C) by amending paragraph (6) to read as follows:

''(6) GAO REVIEW.—Not later than four years after the date of the enactment of this paragraph and every four years thereafter until the termination of the State and Local Cybersecurity Grant Program, the Comptroller General of the United States shall conduct a review of the Program, including relating to the following:

''(A) The grant selection process of the Secretary.

''(B) A sample of grants awarded under this section.

''(C) A review of artificial intelligence adoption across the sample of grants reviewed.'';

(15) in subsection (s), as so redesignated, by amending paragraph (1) to read as follows:

''(1) IN GENERAL.—The activities under this section are subject to the availability of appropriations.''; and

(16) in subsection (t), as so redesignated, in paragraph (1), by striking ''2025'' and inserting ''2035''.