

.....
(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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Protecting Information
5 by Local Leaders for Agency Resilience Act” or the “PIL-
6 LAR Act”.

1 **SEC. 2. REAUTHORIZATION OF CISA STATE AND LOCAL CY-**
2 **BERSECURITY GRANT PROGRAM.**

3 Section 2220A of the Homeland Security Act of 2002
4 (6 U.S.C. 665g) is amended—

5 (1) in subsection (a)—

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

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

11 “(1) **ARTIFICIAL INTELLIGENCE.**—The term
12 ‘artificial intelligence’ has the meaning given such
13 term in section 5002(3) of the National Artificial In-
14 telligence Initiative Act of 2020 (enacted as division
15 E of the William M. (Mac) Thornberry National De-
16 fense Authorization Act for Fiscal Year 2021 (15
17 U.S.C. 9401(3))).

18 “(2) **ARTIFICIAL INTELLIGENCE SYSTEM.**—The
19 term ‘artificial intelligence system’ means any data
20 system, software, hardware, application tool, or util-
21 ity that operates in whole or in part using artificial
22 intelligence.”;

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

25 “(5) **FOREIGN ENTITY OF CONCERN.**—The
26 term ‘foreign entity of concern’ has the meaning

1 given such term in section 10634 of the Research
2 and Development, Competition, and Innovation Act
3 (42 U.S.C. 19237; Public Law 117–167; popularly
4 referred to as the ‘CHIPS and Science Act’).’; and

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

7 “(7) MULTI-FACTOR AUTHENTICATION.—The
8 term ‘multi factor authentication’ means an authen-
9 tication system that requires more than one distinct
10 type of authentication factor for successful authen-
11 tication of a user, including by using a multi-factor
12 authenticator or by combining single-factor authen-
13 ticators that provide different types of factors.”;

14 (2) in subsection (b)(1), by striking “informa-
15 tion systems owned” and inserting “information sys-
16 tems or operational technology systems, including ei-
17 ther or both of such systems using artificial intel-
18 ligence, maintained, owned, or”;

19 (3) in subsection (d)(4), by striking “to the in-
20 formation systems owned” and inserting “to the in-
21 formation systems or operational technology sys-
22 tems, including either or both of such systems using
23 artificial intelligence, maintained, owned, or”; and

24 (4) in subsection (e)—

25 (A) in paragraph (2)—

1 (i) in subparagraph (A)(i), by striking
2 “information systems owned” and insert-
3 ing “information systems or operational
4 technology systems, including either or
5 both of such systems using artificial intel-
6 ligence, maintained, owned, or”;

7 (ii) in subparagraph (B)—

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

10 “(i) manage, monitor, and track appli-
11 cations, user accounts, and information
12 systems and operational technology sys-
13 tems, including either or both of such sys-
14 tems using artificial intelligence, that are
15 maintained, owned, or operated by, or on
16 behalf of, the eligible entity, or, if the eligi-
17 ble entity is a State, local governments
18 within the jurisdiction of the eligible entity,
19 and the information technology deployed
20 on such information systems or operational
21 technology systems (as the case may be),
22 including legacy information systems, oper-
23 ational technology systems, and informa-
24 tion 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;

1 “(iv) implement a process of contin-
2 uous cybersecurity vulnerability assess-
3 ments and threat mitigation practices
4 prioritized by degree of risk to address cy-
5 bersecurity risks and cybersecurity threats
6 on applications, user accounts, and infor-
7 mation systems and operational technology
8 systems, including either or both of such
9 systems using artificial intelligence, main-
10 tained, owned, or operated by, or on behalf
11 of, the eligible entity or, if the eligible enti-
12 ty is a State, local governments within the
13 jurisdiction of the eligible entity;

14 “(v) ensure that the eligible entity
15 and, if the eligible entity is a State, local
16 governments within the jurisdiction of the
17 eligible entity, adopt and use best practices
18 and methodologies to enhance cybersecu-
19 rity, particularly identity and access man-
20 agement solutions such as multi-factor au-
21 thentication, which may include—

22 “(I) the practices set forth in a
23 cybersecurity framework developed by
24 the National Institute of Standards
25 and Technology or the Agency;

1 “(II) cyber chain supply chain
2 risk management best practices iden-
3 tified by the National Institute of
4 Standards and Technology or the
5 Agency;

6 “(III) knowledge bases of adver-
7 sary tools and tactics;

8 “(IV) technologies such as artifi-
9 cial intelligence; and

10 “(V) improving cyber incident re-
11 sponse capabilities through adoption
12 of automated cybersecurity prac-
13 tices;”;

14 (II) in clause (x), by inserting
15 “or operational technology systems,
16 including either or both of such sys-
17 tems using artificial intelligence,”
18 after “information systems”;

19 (III) in clause (xi)(I), by insert-
20 ing “, including through Department
21 of Homeland Security State, Local,
22 and Regional Fusion Center Initiative
23 under section 210(A)” before the
24 semicolon; and

1 (IV) in clause (xii), by inserting
2 “, including for bolstering the resil-
3 ience of outdated or vulnerable infor-
4 mation systems or operational tech-
5 nology systems, including either or
6 both of such systems using artificial
7 intelligence” before the semicolon;

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

10 “(xiii) implement an information tech-
11 nology or operational technology, including
12 either or both of such systems using artifi-
13 cial intelligence, modernization cybersecu-
14 rity review process that ensures alignment
15 between information technology, oper-
16 ational technology, and artificial intel-
17 ligence cybersecurity objectives;”;

18 (VI) in clause (xiv)(II)—

19 (aa) in item (aa), by striking
20 “and” after the semicolon;

21 (bb) in item (bb), by insert-
22 ing “and” after the semicolon;
23 and

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

1 “(cc) academic and non-
2 profit entities, including cyberse-
3 curity clinics and other nonprofit
4 technical assistance programs;”;
5 and

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

8 “(xv) ensure adequate access to, and
9 participation in, the services and programs
10 described in this subparagraph by rural
11 areas and other local governments with
12 small populations within the jurisdiction of
13 the eligible entity, including by direct out-
14 reach to such rural areas and local govern-
15 ments with small populations; and”; and

16 (iii) in subparagraph (F)—

17 (I) in clause (i), by striking
18 “and” after the semicolon;

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

21 “(ii) reducing cybersecurity risks to,
22 and identifying, responding to, and recov-
23 ering from cybersecurity threats to, infor-
24 mation systems or operational technology
25 systems, including either or both of such

1 systems using artificial intelligence, main-
2 tained, owned or operated by, or on behalf
3 of, the eligible entity or, if the eligible enti-
4 ty is a State, local governments within the
5 jurisdiction of the eligible entity; and”;

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

8 “(iii) assuming the cost or partial cost
9 of cybersecurity investments made as a re-
10 sult of the plan.”; and

11 (B) in paragraph (3)(A), by striking “the
12 Multi-State Information Sharing and Analysis
13 Center” and inserting “Information Sharing
14 and Analysis Organizations”;

15 (5) in subsection (g)—

16 (A) in paragraph (2)(A)(ii), by inserting
17 “including, as appropriate, representatives of
18 rural, suburban, and high-population jurisdic-
19 tions (including such jurisdictions with low or
20 otherwise limited operating budgets)” before
21 the semicolon; and

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

24 “(5) RULE OF CONSTRUCTION REGARDING CON-
25 TROL OF CERTAIN INFORMATION SYSTEMS OR OPER-

1 ATIONAL TECHNOLOGY SYSTEMS OF ELIGIBLE ENTI-
2 TIES.—Nothing in this subsection may be construed
3 to permit a cybersecurity planning committee of an
4 eligible entity that meets the requirements of this
5 subsection to make decisions relating to information
6 systems or operational technology systems, including
7 either or both of such systems using artificial intel-
8 ligence, maintained, owned, or operated by, or on be-
9 half of, the eligible entity.”;

10 (6) in subsection (i)—

11 (A) in paragraph (1)(B), by striking “2-
12 year period” and inserting “3-year period”;

13 (B) in paragraph (3)—

14 (i) in the matter preceding subpara-
15 graph (A), by striking “2023” and insert-
16 ing “2027”; and

17 (ii) in subparagraph (B), by striking
18 “2023” and inserting “2027”; and

19 (C) in paragraph (4)—

20 (i) in the matter preceding subpara-
21 graph (A), by striking “shall” and insert-
22 ing “may”; and

23 (ii) in subparagraph (A), by striking
24 “information systems owned” inserting
25 “information systems or operational tech-

1 nology systems, including either or both of
2 such systems using artificial intelligence,
3 maintained, owned,”;

4 (7) in subsection (j)(1)—

5 (A) in subparagraph (D), by striking “or”
6 after the semicolon;

7 (B) in subparagraph (E)—

8 (i) by striking “information systems
9 owned” and inserting “information sys-
10 tems or operational technology systems, in-
11 cluding either or both of such systems
12 using artificial intelligence, maintained,
13 owned,”; and

14 (ii) by striking the period and insert-
15 ing a semicolon; and

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

18 “(E) to purchase software or hardware, or
19 products or services of such software or hard-
20 ware, as the case may be, that do not align with
21 guidance relevant to such software or hardware,
22 or products or services, as the case may be, pro-
23 vided by the Agency, including Secure by De-
24 sign or successor guidance; or

1 “(F) to purchase software or hardware, or
2 products or services of such software or hard-
3 ware, as the case may be, that are designed, de-
4 veloped, operated, maintained, manufactured, or
5 sold by a foreign entity of concern and do not
6 align with guidance provided by the Agency.”;

7 (8) in subsection (l), in the matter preceding
8 paragraph (1), by striking “2022” and inserting
9 “2026”;

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

12 “(1) IN GENERAL.—The Federal share of ac-
13 tivities carried out using funds made available pur-
14 suant to the award of a grant under this section
15 may not exceed—

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

19 “(B) in the case of a grant to a multi-enti-
20 ty group, 70 percent for each fiscal year
21 through fiscal year 2035.

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

1 cal year beginning with fiscal year 2028 through fis-
2 cal year 2035 if such entity or multi-entity group
3 entity, as the case may be, implements or enables,
4 by not later than October 1, 2027, multi-factor au-
5 thentication and identity and access management
6 tools that support multi-factor authentication with
7 respect to critical infrastructure, including the infor-
8 mation systems and operational technology systems,
9 including either or both of such systems using artifi-
10 cial intelligence, of such critical infrastructure, that
11 is within the jurisdiction of such entity or multi-enti-
12 ty group is responsible.”;

13 (10) in subsection (n)—

14 (A) in paragraph (2)—

15 (i) in subparagraph (A)—

16 (I) in the matter preceding clause

17 (i), by striking “a grant” and insert-

18 ing “a grant on or after January 1,

19 2026, or changes the allocation of

20 funding as permissible within the al-

21 lowances of”; and

22 (II) by amending clauses (ii) and

23 (iii) to read as follows:

24 “(ii) with the consent of the local gov-

25 ernments, items, in-kind services, capabili-

1 ties, or activities, or a combination of fund-
2 ing and other services, having a value of
3 not less than 80 percent of the amount of
4 the grant; or

5 “(iii) with the consent of the local
6 governments, grant funds combined with
7 other items, in-kind services, capabilities,
8 or activities, or a combination of funding
9 and other services, having the total value
10 of not less than 80 percent of the amount
11 of the grant.”; and

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

14 “(ii) items, in kind services, capabili-
15 ties, or activities, or a combination of fund-
16 ing and other services, having a value of
17 not less than 25 percent of the amount of
18 the grant awarded to the eligible entity; or

19 “(iii) grant funds combined with other
20 items, in kind services, capabilities, or ac-
21 tivities, or a combination of funding and
22 other services, having the total value of not
23 less than 25 percent of the grant awarded
24 to the eligible entity.”; and

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

3 “(5) DIRECT FUNDING.—If an eligible entity
4 does not make a distribution to a local government
5 required under paragraph (2) within 60 days of the
6 anticipated grant disbursement date, such local gov-
7 ernment may petition the Secretary to request the
8 Secretary to provide funds directly to such local gov-
9 ernment.”;

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

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

16 (13) by inserting after subsection (o) the fol-
17 lowing new subsection:

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

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

24 (A) in paragraph (1)(A)—

1 (i) in clause (i), by striking “and”
2 after the semicolon;

3 (ii) in clause (ii)—

4 (I) by striking “information sys-
5 tems owned” inserting “information
6 systems or operational technology sys-
7 tems, including either or both of such
8 systems using artificial intelligence,
9 maintained, owned,”; and

10 (II) by striking the period and
11 inserting “; and”; and

12 (iii) by adding at the end the fol-
13 lowing new clause:

14 “(iii) assuming the costs associated
15 with continuing the programs specified in
16 the Cybersecurity Plan by including such
17 programs in State and local government
18 budgets upon full expenditure of grant
19 funds by the eligible entity.”;

20 (B) in paragraph (2)(E)(ii), by striking
21 “information systems owned” and inserting “in-
22 formation systems or operational technology
23 systems, including either or both of such sys-
24 tems using artificial intelligence, maintained,
25 owned”; and

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

3 “(6) GAO REVIEW.—Not later than four years
4 after the date of the enactment of this paragraph
5 and every four years thereafter until the termination
6 of the State and Local Cybersecurity Grant Pro-
7 gram, the Comptroller General of the United States
8 shall conduct a review of the Program, including re-
9 lating to the following:

10 “(A) The grant selection process of the
11 Secretary.

12 “(B) A sample of grants awarded under
13 this section.

14 “(C) A review of artificial intelligence
15 adoption across the sample of grants re-
16 viewed.”;

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

19 “(1) IN GENERAL.—The activities under this
20 section are subject to the availability of appropria-
21 tions.”; and

22 (16) in subsection (t), as so redesignated, in
23 paragraph (1), by striking “2025” and inserting
24 “2035”.