

119TH CONGRESS
1ST SESSION

H. R. 5078

IN THE SENATE OF THE UNITED STATES

NOVEMBER 18, 2025

Received; read twice and referred to the Committee on Homeland Security and
Governmental Affairs

AN ACT

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,*

1 **SECTION 1. SHORT TITLE.**

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

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

7 Section 2220A of the Homeland Security Act of 2002
8 (6 U.S.C. 665g) is amended—

9 (1) in subsection (a)—

10 (A) by redesignating paragraphs (1), (2),
11 (3), (4), (5), (6), and (7) as paragraphs (3),
12 (4), (6), (8), (9), (10), and (11), respectively;

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

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

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

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

3 “(5) FOREIGN ENTITY OF CONCERN.—The
4 term ‘foreign entity of concern’ has the meaning
5 given such term in section 10634 of the Research
6 and Development, Competition, and Innovation Act
7 (42 U.S.C. 19237; Public Law 117–167; popularly
8 referred to as the ‘CHIPS and Science Act’).”; and

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

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

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

23 (3) in subsection (d)(4), by striking “to the in-
24 formation systems owned” and inserting “to the in-
25 formation systems or operational technology sys-

tems, including either or both of such systems using
artificial intelligence, maintained, owned,”;

(4) in subsection (e)—

(A) in paragraph (2)—

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

(ii) in subparagraph (B)—

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

“(i) manage, monitor, and track appli-
cations, user accounts, and information
systems and operational technology sys-
tems, including either or both of such sys-
tems using artificial intelligence, that are
maintained, owned, or operated by, or on
behalf of, the eligible entity, or, if the eligi-
ble 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),

1 including legacy information systems, oper-
2 ational technology systems, and informa-
3 tion technology that are no longer sup-
4 ported by the manufacturer of the systems
5 or technology at issue;

6 “(ii) monitor, audit, and track net-
7 work traffic and activity transiting or trav-
8 eling to or from applications, user ac-
9 counts, and information systems and oper-
10 ational technology systems, including either
11 or both of such systems using artificial in-
12 telligence, maintained, owned, or operated
13 by, or on behalf of, the eligible entity or,
14 if the eligible entity is a State, local gov-
15 ernments within the jurisdiction of the eli-
16 gible entity;

17 “(iii) enhance the preparation, re-
18 sponse, and resiliency of applications, user
19 accounts, and information systems and
20 operational technology systems, including
21 either or both of such systems using artifi-
22 cial intelligence, maintained, owned, or op-
23 erated by, or on behalf of, the eligible enti-
24 ty or, if the eligible entity is a State, local
25 governments within the jurisdiction of the

1 eligible entity, against cybersecurity risks
2 and cybersecurity threats;

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

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

24 “(I) the practices set forth in a
25 cybersecurity framework developed by

1 the National Institute of Standards
2 and Technology or the Agency;

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

8 “(III) knowledge bases of adver-
9 sary tools and tactics;

10 “(IV) technologies such as artifi-
11 cial intelligence; and

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

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

21 (III) in clause (xi)(I), by insert-
22 ing “, including through Department
23 of Homeland Security State, Local,
24 and Regional Fusion Center Initiative

1 under section 210(A)” before the
2 semicolon;

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

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

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

20 (VI) in clause (xiv)(II)—

21 (aa) in item (aa), by striking
22 “and” after the semicolon;

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

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

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

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

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

18 (iii) in subparagraph (F)—

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

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

23 “(ii) reducing cybersecurity risks to,
24 and identifying, responding to, and recov-
25 ering from cybersecurity threats to, infor-

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

8 (III) by adding at the end the

9 following new clause:

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

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

17 (5) in subsection (g)—

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

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

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

12 (6) in subsection (i)—

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

15 (B) in paragraph (3)—

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

19 (ii) in subparagraph (B), by striking
20 “2023” and inserting “2027”; and

21 (C) in paragraph (4)—

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

1 (ii) in subparagraph (A), 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,”;

7 (7) in subsection (j)(1)—

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

10 (B) in subparagraph (E)—

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

17 (ii) by striking the period and insert-
18 ing a semicolon; and

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

21 “(F) to purchase software or hardware, or
22 products or services of such software or hard-
23 ware, as the case may be, that do not align with
24 guidance relevant to such software or hardware,
25 or products or services, as the case may be, pro-

1 vided by the Agency, including Secure by De-
2 sign or successor guidance; or

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

9 (8) in subsection (l), in the matter preceding
10 paragraph (1), by striking “2022” and inserting
11 “2026”;

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

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

18 “(A) in the case of a grant to an eligible
19 entity, 60 percent for each fiscal year through
20 fiscal year 2033; and

21 “(B) in the case of a grant to a multi-enti-
22 ty group, 70 percent for each fiscal year
23 through fiscal year 2033.

24 Notwithstanding subparagraphs (A) and (B), the
25 Federal share of the cost for an eligible entity or

1 multi-entity group shall be 65 percent for an entity
2 and 75 percent for a multi-group entity for each fis-
3 cal year beginning with fiscal year 2028 through fis-
4 cal year 2033 if such entity or multi-entity group
5 entity, as the case may be, implements or enables,
6 by not later than October 1, 2027, multi-factor au-
7 thentication and identity and access management
8 tools that support multi-factor authentication with
9 respect to critical infrastructure, including the infor-
10 mation systems and operational technology systems,
11 including either or both of such systems using artifi-
12 cial intelligence, of such critical infrastructure, that
13 is within the jurisdiction of such entity or multi-enti-
14 ty group is responsible.”;

15 (10) in subsection (n)—

16 (A) in paragraph (2)—

17 (i) in subparagraph (A)—

18 (I) in the matter preceding clause

19 (i), by striking “a grant” and insert-
20 ing “a grant on or after January 1,
21 2026, or changes the allocation of
22 funding as permissible within the al-
23 lowances”; and

24 (II) by amending clauses (ii) and

25 (iii) to read as follows:

1 “(ii) with the consent of the local gov-
2 ernments, items, in-kind services, capabili-
3 ties, or activities, or a combination of fund-
4 ing and other services, having a value of
5 not less than 80 percent of the amount of
6 the grant; or

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

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

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

21 “(iii) grant funds combined with other
22 items, in kind services, capabilities, or ac-
23 tivities, or a combination of funding and
24 other services, having the total value of not

1 less than 25 percent of the grant awarded
2 to the eligible entity.”; and

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

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

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

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

18 (13) by inserting after subsection (o) the fol-
19 lowing new subsection:

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

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

1 (A) in paragraph (1)(A)—

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

4 (ii) in clause (ii)—

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

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

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

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

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

1 tems using artificial intelligence, maintained,
2 owned”; and

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

5 “(6) GAO REVIEW.—Not later than three years
6 after the date of the enactment of this paragraph
7 and every three years thereafter until the termi-
8 nation of the State and Local Cybersecurity Grant
9 Program, the Comptroller General of the United
10 States shall conduct a review of the Program, in-
11 cluding relating to the following:

12 “(A) The grant selection process of the
13 Secretary.

14 “(B) A sample of grants awarded under
15 this section.

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

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

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

Attest: KEVIN F. MCCUMBER,
Clerk.