

119TH CONGRESS
1ST SESSION

H. R. 5079

To reauthorize the Cybersecurity Act of 2015, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 2, 2025

Mr. GARBARINO (for himself and Mr. MCCAUL) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Oversight and Government Reform, Intelligence (Permanent Select), Energy and Commerce, Armed Services, and the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To reauthorize the Cybersecurity Act of 2015, 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 “Widespread Informa-
5 tion Management for the Welfare of Infrastructure and
6 Government Act”.

1 **SEC. 2. REAUTHORIZATION OF CYBERSECURITY ACT OF**
2 **2015.**

3 (a) IN GENERAL.—The Cybersecurity Act of 2015 (6
4 U.S.C. 1501 et seq.; enacted as division N of the Consoli-
5 dated Appropriations Act, 2016; Public Law 114–113) is
6 amended—

7 (1) in section 102 (6 U.S.C. 1501; relating to
8 definitions)—

9 (A) by redesignating paragraphs (4), (5),
10 (6), (7), (8), (9), (10), (11), (12), (13), (14),
11 (15), (16), (17), and (18) as paragraphs (6),
12 (7), (8), (9), (10), (11), (12), (13), (14), (15),
13 (16), (17), (19), (20), and (21), respectively;

14 (B) by inserting after paragraph (3) the
15 following new paragraphs:

16 “(4) **ARTIFICIAL INTELLIGENCE.**—The term
17 ‘artificial intelligence’ has the meaning given such
18 term in section 5002 of the National Artificial Intel-
19 ligence Initiative Act of 2020 (15 U.S.C. 9401).

20 “(5) **CRITICAL INFRASTRUCTURE.**—The term
21 ‘critical infrastructure’ has the meaning given such
22 term in section 1016(e) of Public Law 107–56 (42
23 U.S.C. 5195c(e)).”; and

24 (C) by inserting after paragraph (17), as
25 so redesignated, the following new paragraph:

1 “(18) SECTOR RISK MANAGEMENT AGENCY.—

2 The term ‘Sector Risk Management Agency’ has the
3 meaning given such term in section 2200 of the
4 Homeland Security Act of 2002 (6 U.S.C. 650).”;

5 (2) in section 103 (6 U.S.C. 1502; relating to
6 sharing of information by the Federal Govern-
7 ment)—

8 (A) in subsection (a), in the matter pre-
9 ceding paragraph (1), by striking “develop and
10 issue” and inserting “develop, issue, and, as ap-
11 propriate, update”;

12 (B) in subsection (b)—

13 (i) in paragraph (1)—

14 (I) in the matter preceding sub-
15 paragraph (A), by inserting “and, as
16 appropriate, updated,” after “devel-
17 oped”;

18 (II) by amending subparagraph

19 (A) to read as follows:

20 “(A) ensure the Federal Government main-
21 tains the capability to provide technical assist-
22 ance, on a voluntary basis, to non-Federal enti-
23 ties in utilizing cyber threat indicators and de-
24 fensive measures for cybersecurity purposes.”;

1 (III) in subparagraph (E)(ii), by
2 striking “and” after the semicolon;

3 (IV) in subparagraph (F), by
4 striking the period and inserting “;
5 and”; and

6 (V) by adding at the end the fol-
7 lowing new subparagraph:

8 “(G) pursuant to section 2212 of the
9 Homeland Security Act of 2002 (6 U.S.C. 662),
10 provide one-time read-ins, as appropriate, to se-
11 lect individuals identified by non-Federal enti-
12 ties that own or operate critical infrastruc-
13 ture;”; and

14 (ii) in paragraph (2)—

15 (I) by inserting “and, as appro-
16 priate, updating,” after “developing”;
17 and

18 (II) by inserting “and defensive
19 measures” after “promote the sharing
20 of cyber threat indicators”; and

21 (C) in subsection (c)—

22 (i) by inserting “and not later than 60
23 days after any update, as appropriate, of
24 procedures required by subsection (a),”
25 after “Act,”; and

1 (ii) by inserting “(or update, as ap-
2 propriate)” after “procedures”;

3 (3) in section 104 (6 U.S.C. 1503; relating to
4 authorizations for preventing, detecting, analyzing,
5 and mitigating cybersecurity threats)—

6 (A) in subsection (c)—

7 (i) in paragraph (1), by inserting “,
8 including Sector Risk Management Agen-
9 cies that are agencies and the majority of
10 the systems of which are not covered under
11 subsection (d) or (e) of section 3553 of
12 title 44, United States Code,” after “Fed-
13 eral Government”;

14 (ii) in paragraph (3)—

15 (I) in the matter preceding sub-
16 paragraph (A), by striking “shall be”
17 and inserting “may be”;

18 (II) in subparagraph (A), by
19 striking “or” after the semicolon;

20 (III) in subparagraph (B), by
21 striking the period and inserting “;
22 or”; and

23 (IV) by adding at the end the fol-
24 lowing new subparagraph:

“(C) to preclude the use of artificial intelligence that is developed or strictly deployed for cybersecurity purposes in carrying out the activities authorized under paragraph (1).”; and

(iii) in subparagraph (B) of subsection (d)(2), by inserting “, which may utilize artificial intelligence that is developed or strictly deployed for cybersecurity purposes,” after “technical capability”;

(4) in section 105 (6 U.S.C. 1504); relating to sharing of cyber threat indicators and defensive measures with the Federal Government—

(A) in subsection (a)—

(i) in paragraph (2), by adding at the end the following new sentences: “As appropriate, the Attorney General and the Secretary of Homeland Security shall, in consultation with the heads of the appropriate Federal entities, jointly update such policies and procedures, and issue and make publicly available such updated policies and procedures. Such updates shall prioritize rapid dissemination to State, local, Tribal, and territorial governments and owners and operators of non-Federal

critical infrastructure of relevant and actionable cyber threat indicators and defensive measures.”;

(ii) in paragraph (3), in the matter preceding subparagraph (A), by striking “developed or issued” and inserting “developed, issued, or, as appropriate, updated,”; and

(iii) in paragraph (4)—

(I) in subparagraph (A), by adding at the end the following new sentence: “As appropriate, the Attorney General and the Secretary of Homeland Security shall jointly update and make publicly available such guidance to so assist entities and promote such sharing of cyber threat indicators and defensive measures with such Federal entities under this title.”; and

(II) in subparagraph (B), in the matter preceding clause (i), by inserting “and, as appropriate, updated,” after “developed”;

(B) in subsection (b)—

1 (i) in paragraph (2)(B), by inserting
2 “, and, as appropriate, update,” after “re-
3 view”; and

4 (ii) in paragraph (3), in the matter
5 preceding subparagraph (A), by inserting
6 “and, as appropriate, updated,” after “re-
7 quired”;

8 (C) in subsection (c)—

9 (i) in paragraph (1)(D), by inserting
10 “, including if such capability and process
11 employs artificial intelligence” before the
12 semicolon;

13 (ii) in paragraph (2), by adding at the
14 end the following new subparagraph:

15 “(C) OUTREACH.—Not later than 90 days
16 after the date of the enactment of this subpara-
17 graph, the Secretary of Homeland Security
18 shall develop and continuously implement an
19 outreach plan, including targeted engagement,
20 to ensure Federal and non-Federal entities,
21 particularly small or rural owners or operators
22 of critical infrastructure which often lack dedi-
23 cated cybersecurity staff but remain vital to na-
24 tional security—

1 “(i) are aware of the capability and
2 process required by paragraph (1) to share
3 cyber threat indicators and defensive meas-
4 ures, including the benefits real-time infor-
5 mation sharing provides;

6 “(ii) understand how to share cyber
7 threat indicators and defensive measures;

8 “(iii) understand the obligation to re-
9 move certain personal information in ac-
10 cordance with section 104(d)(7) prior to
11 sharing a cyber threat indicator;

12 “(iv) understand how cyber threat in-
13 dicators and defensive measures are re-
14 ceived, processed, used, and protected;

15 “(v) understand the protections they
16 are afforded in sharing any cyber threat
17 indicators and defensive measures; and

18 “(vi) can provide feedback to the Sec-
19 retary when policies, procedures, and
20 guidelines that are unclear or unintention-
21 ally prohibitive to sharing cyber threat in-
22 dicators and defensive measures.”; and

23 (iii) by adding at the end the fol-
24 lowing new subparagraph:

1 “(D) BRIEFINGS ON OUTREACH.—The
2 Secretary of Homeland Security shall annually
3 provide to the Committee on Homeland Security
4 of the House of Representatives and the
5 Committee on Homeland Security and Governmental
6 Affairs of the Senate a briefing on the
7 implementation of outreach pursuant to sub-
8 paragraph (B).”; and

9 (D) in subsection (d)—

10 (i) in paragraph (1), by inserting
11 “copyright or” before “trade secret protec-
12 tion”; and

13 (ii) in paragraph (5)(A),

14 (I) in clause (iv), by striking
15 “or” after the semicolon;

16 (II) in clause (v)(III), by striking
17 the period and inserting “; or”; and

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

20 “(vi) the purpose of rapidly providing
21 other Federal entities, including Sector
22 Risk Management Agencies, awareness of
23 a cybersecurity threat that may impact the
24 information systems of such Agencies.”;

1 (5) in section 108 (6 U.S.C. 1507; relating to
2 construction and preemption)—

3 (A) in subsection (c)—

4 (i) in the matter preceding paragraph
5 (1), by striking “shall be” and inserting
6 “may be”;

7 (ii) in paragraph (2), by striking “or”
8 after the semicolon;

9 (iii) in paragraph (3), by striking the
10 period and inserting “; or”; and

11 (iv) by adding at the end the following
12 new paragraph:

13 “(4) to preclude the use of artificial intelligence
14 that is developed or strictly deployed for cybersecu-
15 rity purposes in carrying out activities authorized by
16 this title.”; and

17 (B) in subsection (f)—

18 (i) in paragraph (3)—

19 (I) by inserting “to share cyber
20 threat indicators or defensive meas-
21 ures” after “relationship”; and

22 (II) by striking “or” after the
23 semicolon;

24 (ii) in paragraph (4), by striking the
25 period and inserting “; or”; and

1 (iii) by adding at the end the fol-
2 lowing new paragraph:

3 “(5) to limit or modify, notwithstanding any
4 other provision of law, the authorization to share
5 pursuant to section 104(c)(1) with Sector Risk Man-
6 agement Agencies described in such section.”;

7 (6) in section 109 (6 U.S.C. 1508; relating to
8 report on cybersecurity threats)—

9 (A) in subsection (a)—

10 (i) by inserting “and not later than
11 September 30 of every two years there-
12 after,” after “Act,”;

13 (ii) by inserting “the Secretary of
14 Homeland Security and” after “in coordi-
15 nation with”;

16 (iii) by inserting “and the Committee
17 on Homeland Security and Governmental
18 Affairs” before “of the Senate”;

19 (iv) by inserting “and the Committee
20 on Homeland Security” before “of the
21 House”; and

22 (v) by inserting “prepositioning activi-
23 ties, ransomware,” after “attacks,”; and

24 (B) in subsection (b)—

1 (i) in paragraph (1), by inserting
2 “prepositioning activities, ransomware,”
3 after “attacks,”;

4 (i) in paragraph (2), by inserting
5 “prepositioning activity, ransomware,”
6 after “attack,”;

7 (i) in paragraph (3), by inserting
8 “prepositioning activities, ransomware,”
9 after “attacks,” each place it appears; and

10 (i) in paragraph (4), by inserting
11 “prepositioning activities, ransomware,”
12 after “attacks,”; and

13 (7) in section 111(a) (6 U.S.C. 1510(a), relat-
14 ing to effective period), by striking “2025” and in-
15 serting “2035”.

16 (b) CONFORMING AMENDMENTS.—Section 2200 of
17 the Homeland Security Act of 2002 (6 U.S.C. 650; relat-
18 ing to definitions) is amended—

19 (1) in paragraph (5)—

20 (A) in subparagraph (B), by inserting “or
21 compromising” after “defeating”;

22 (B) in subparagraph (C), by inserting “in-
23 cluding a security vulnerability affecting an in-
24 formation system or a technology included in
25 the critical and emerging technologies list of the

1 Office of Science and Technology Policy or suc-
2 cessor list, such as artificial intelligence (as
3 such term is defined in section 5002 of the Na-
4 tional Artificial Intelligence Initiative Act of
5 2020 (15 U.S.C. 9401)), which may be in a
6 Federal entity's or non-Federal entity's soft-
7 ware or hardware supply chain," after "security
8 vulnerability,";

9 (C) in subparagraph (D), by inserting "or
10 compromise" after "defeat"; and

11 (D) in subparagraph (F), by inserting "or
12 compromised" after "exfiltrated";

13 (2) in paragraph (14), by amending subpara-
14 graph (B) to read as follows:

15 "(B) includes, in accordance with section
16 104(d)(2) of the Cybersecurity Sharing Act of
17 2015 (6 U.S.C. 1503(d)(2))—

18 "(i) operational technology, including
19 industrial control systems, such as super-
20 visory control and data acquisition sys-
21 tems, distributed control systems, and pro-
22 grammable logic controllers;

23 "(ii) edge devices; and

1 “(iii) internet of things devices, in-
2 cluding digital and physical infrastructure
3 impacted by ransomware.”; and
4 (3) in paragraph (25), by inserting “or com-
5 promise” after “defeat”.

○