## AMENDMENT IN THE NATURE OF A SUBSTITUTE TO H.R. 5079

## OFFERED BY MR. GARBARINO OF NEW YORK

Strike all after the enacting clause and insert the following:

## 1 SECTION 1. SHORT TITLE.

- 2 This Act may be cited as the "Widespread Informa-
- 3 tion Management for the Welfare of Infrastructure and
- 4 Government Act".
- 5 SEC. 2. REAUTHORIZATION OF THE CYBERSECURITY ACT
- 6 **OF 2015.**
- 7 (a) In General.—The Cybersecurity Act of 2015 (6
- 8 U.S.C. 1501 et seq.; enacted as division N of the Consoli-
- 9 dated Appropriations Act, 2016; Public Law 114–113) is
- 10 amended—
- 11 (1) in section 102 (6 U.S.C. 1501; relating to
- definitions)—
- (A) by redesignating paragraphs (4), (5),
- (6), (7), (8), (9), (10), (11), (12), (13), (14),
- 15 (15), (16), (17), and (18) as paragraphs (6),
- (7), (8), (9), (10), (11), (12), (13), (14), (15),
- 17 (16), (17), (19), (20), and (21), respectively;

1	(B) by inserting after paragraph (3) the
2	following new paragraphs:
3	"(4) Artificial intelligence.—The term
4	'artificial intelligence' has the meaning given such
5	term in section 5002 of the National Artificial Intel-
6	ligence Initiative Act of 2020 (15 U.S.C. 9401).
7	"(5) Critical infrastructure.—The term
8	'critical infrastructure' has the meaning given such
9	term in section 1016(e) of Public Law 107–56 (42
10	U.S.C. 5195c(e))."; and
11	(C) by inserting after paragraph (17), as
12	so redesignated, the following new paragraph:
13	"(18) Sector risk management agency.—
14	The term 'Sector Risk Management Agency' has the
15	meaning given such term in section 2200 of the
16	Homeland Security Act of 2002 (6 U.S.C. 650).";
17	(2) in section 103 (6 U.S.C. 1502; relating to
18	sharing of information by the Federal Govern-
19	ment)—
20	(A) in subsection (a), in the matter pre-
21	ceding paragraph (1), by striking "develop and
22	issue" and inserting "develop, issue, and, as ap-
23	propriate, update"; and
24	(B) in subsection (b)—
25	(i) in paragraph (1)—

1	(I) in the matter preceding sub-
2	paragraph (A), by inserting "and, as
3	appropriate, updated," after "devel-
4	oped'';
5	(II) by amending subparagraph
6	(A) to read as follows:
7	"(A) ensure the Federal Government main-
8	tains the capability to provide technical assist-
9	ance, on a voluntary basis, to non-Federal enti-
10	ties in utilizing cyber threat indicators and de-
11	fensive measures for cybersecurity purposes;";
12	(III) in subparagraph (E)(ii), by
13	striking "and" after the semicolon;
14	(IV) in subparagraph (F), by
15	striking the period and inserting ";
16	and"; and
17	(V) by adding at the end the fol-
18	lowing new subparagraph:
19	"(G) pursuant to section 2212 of the
20	Homeland Security Act of 2002 (6 U.S.C. 662),
21	provide one-time read-ins, as appropriate, to se-
22	lect individuals identified by non-Federal enti-
23	ties that own or operate critical infrastruc-
24	ture;"; and
25	(ii) in paragraph (2)—

1	(I) by inserting "and, as appro-
2	priate, updating," after "developing";
3	and
4	(II) by inserting "and defensive
5	measures" after "promote the sharing
6	of cyber threat indicators"; and
7	(C) in subsection (c)—
8	(i) by inserting "and not later than 60
9	days after any update, as appropriate, of
10	procedures required by subsection (a),"
11	after "Act,"; and
12	(ii) by inserting "(or update, as ap-
13	propriate)" after "procedures";
14	(3) in section 104 (6 U.S.C. 1503; relating to
15	authorizations for preventing, detecting, analyzing,
16	and mitigating cybersecurity threats)—
17	(A) in subsection (c)—
18	(i) in paragraph (1), by inserting ",
19	including Sector Risk Management Agen-
20	cies that are agencies and the majority of
21	the systems of which are not covered under
22	subsection (d) or (e) of section 3553 of
23	title 44, United States Code," after "Fed-
24	eral Government''; and
25	(ii) in paragraph (3)—

1	(I) in the matter preceding sub-
2	paragraph (A), by striking "shall be"
3	and inserting "may be";
4	(II) in subparagraph (A), by
5	striking "or" after the semicolon;
6	(III) in subparagraph (B), by
7	striking the period and inserting ";
8	or''; and
9	(IV) by adding at the end the fol-
10	lowing new subparagraph:
11	"(C) to preclude the use of artificial intel-
12	ligence that is developed or strictly deployed for
13	cybersecurity purposes in carrying out the ac-
14	tivities authorized under paragraph (1)."; and
15	(iii) in subparagraph (B) of sub-
16	section $(d)(2)$ , by inserting ", which may
17	utilize artificial intelligence that is devel-
18	oped or strictly deployed for cybersecurity
19	purposes," after "technical capability";
20	(4) in section 105 (6 U.S.C. 1504); relating to
21	sharing of cyber threat indicators and defensive
22	measures with the Federal Government)—
23	(A) in subsection (a)—
24	(i) in paragraph (2), by adding at the
25	end the following new sentences: "As ap-

1	propriate, the Attorney General and the
2	Secretary of Homeland Security shall, in
3	consultation with the heads of the appro-
4	priate Federal entities, jointly update such
5	policies and procedures, and issue and
6	make publicly available such updated poli-
7	cies and procedures. Such updates shall
8	prioritize rapid dissemination to State,
9	local, Tribal, and territorial governments
10	and owners and operators of non-Federal
11	critical infrastructure of relevant and ac-
12	tionable cyber threat indicators and defen-
13	sive measures.";
14	(ii) in paragraph (3), in the matter
15	preceding subparagraph (A), by striking
16	"developed or issued" and inserting "devel-
17	oped, issued, or, as appropriate, updated,";
18	and
19	(iii) in paragraph (4)—
20	(I) in subparagraph (A), by add-
21	ing at the end the following new sen-
22	tence: "As appropriate, the Attorney
23	General and the Secretary of Home-
24	land Security shall jointly update and
25	make publicly available such guidance

1	to so assist entities and promote such
2	sharing of cyber threat indicators and
3	defensive measures with such Federal
4	entities under this title."; and
5	(II) in subparagraph (B), in the
6	matter preceding clause (i), by insert-
7	ing "and, as appropriate, updated,"
8	after "developed";
9	(B) in subsection (b)—
10	(i) in paragraph (2)(B), by inserting
11	", and, as appropriate, update," after "re-
12	view"; and
13	(ii) in paragraph (3), in the matter
14	preceding subparagraph (A), by inserting
15	"and, as appropriate, updated," after "re-
16	quired"; and
17	(C) in subsection (c)—
18	(i) in paragraph (1)(D), by inserting
19	", including if such capability and process
20	employs artificial intelligence" before the
21	semicolon; and
22	(ii) in paragraph (2), by adding at the
23	end the following new subparagraph:
24	"(C) Outreach.—Not later than 90 days
25	after the date of the enactment of this subpara-

1	graph, the Secretary of Homeland Security
2	shall develop and continuously implement an
3	outreach plan, including targeted engagement,
4	to ensure Federal and non-Federal entities,
5	particularly small or rural owners or operators
6	of critical infrastructure which often lack dedi-
7	cated cybersecurity staff but remain vital to na-
8	tional security—
9	"(i) are aware of the capability and
10	process required by paragraph (1) to share
11	cyber threat indicators and defensive meas-
12	ures, including the benefits real-time infor-
13	mation sharing provides;
14	"(ii) understand how to share cyber
15	threat indicators and defensive measures;
16	"(iii) understand the obligation to re-
17	move certain personal information in ac-
18	cordance with section 104(d)(7) prior to
19	sharing a cyber threat indicator;
20	"(iv) understand how cyber threat in-
21	dicators and defensive measures are re-
22	ceived, processed, used, and protected;
23	"(v) understand the protections they
24	are afforded in sharing any cyber threat
25	indicators and defensive measures; and

1	"(vi) can provide feedback to the Sec-
2	retary when policies, procedures, and
3	guidelines that are unclear or unintention-
4	ally prohibitive to sharing cyber threat in-
5	dicators and defensive measures."; and
6	(iii) by adding at the end the fol-
7	lowing new subparagraph:
8	"(D) Briefings on outreach.—The
9	Secretary of Homeland Security shall annually
10	provide to the Committee on Homeland Secu-
11	rity of the House of Representatives and the
12	Committee on Homeland Security and Govern-
13	mental Affairs of the Senate a briefing on the
14	implementation of outreach pursuant to sub-
15	paragraph (B)."; and
16	(D) in subsection (d)—
17	(i) in paragraph (1), by inserting
18	"copyright or" before "trade secret protec-
19	tion'; and
20	(ii) in paragraph (5)(A),
21	(I) in clause (iv), by striking
22	"or" after the semicolon;
23	(II) in clause (v)(III), by striking
24	the period and inserting "; or"; and

1	(III) by adding at the end the
2	following new clause:
3	"(vi) the purpose of rapidly providing
4	other Federal entities, including Sector
5	Risk Management Agencies, awareness of
6	a cybersecurity threat that may impact the
7	information systems of such Agencies.";
8	(5) in section 108 (6 U.S.C. 1507; relating to
9	construction and preemption)—
10	(A) in subsection (e)—
11	(i) in the matter preceding paragraph
12	(1), by striking "shall be" and inserting
13	"may be";
14	(ii) in paragraph (2), by striking "or"
15	after the semicolon;
16	(iii) in paragraph (3), by striking the
17	period and inserting "; or"; and
18	(iv) by adding at the end the following
19	new paragraph:
20	"(4) to preclude the use of artificial intelligence
21	that is developed or strictly deployed for cybersecu-
22	rity purposes in carrying out activities authorized by
23	this title.";
24	(B) in subsection (f)—
25	(i) in paragraph (3)—

1	(I) by inserting "to share cyber
2	threat indicators or defensive meas-
3	ures" after "relationship"; and
4	(II) by striking "or" after the
5	semicolon;
6	(ii) in paragraph (4), by striking the
7	period and inserting "; or"; and
8	(iii) by adding at the end the fol-
9	lowing new paragraph:
10	"(5) to limit or modify, notwithstanding any
11	other provision of law, the authorization to share
12	pursuant to section $104(c)(1)$ with Sector Risk Man-
13	agement Agencies described in such section.";
14	(6) in section 109 (6 U.S.C. 1508; relating to
15	report on cybersecurity threats)—
16	(A) in subsection (a)—
17	(i) by inserting "and not later than
18	September 30 of every two years there-
19	after," after "Act,";
20	(ii) by inserting "the Secretary of
21	Homeland Security and" after "in coordi-
22	nation with";
23	(iii) by inserting "and the Committee
24	on Homeland Security and Governmental
25	Affairs" before "of the Senate":

1	(iv) by inserting "and the Committee
2	on Homeland Security' before "of the
3	House"; and
4	(v) by inserting "prepositioning activi-
5	ties, ransomware," after "attacks,"; and
6	(B) in subsection (b)—
7	(i) in paragraph (1), by inserting
8	"prepositioning activities, ransomware,"
9	after "attacks,";
10	(i) in paragraph (2), by inserting
11	"prepositioning activity, ransomware,"
12	after "attack,";
13	(i) in paragraph (3), by inserting
14	"prepositioning activities, ransomware,"
15	after "attacks," each place it appears; and
16	(i) in paragraph (4), by inserting
17	"prepositioning activities, ransomware,"
18	after "attacks,"; and
19	(7) in section 111(a) (6 U.S.C. 1510(a), relat-
20	ing to effective period), by striking "2025" and in-
21	serting "2035".
22	(b) Conforming Amendments.—Section 2200 of
23	the Homeland Security Act of 2002 (6 U.S.C. 650; relat-
24	ing to definitions) is amended—
25	(1) in paragraph (5)—

1	(A) in subparagraph (B), by inserting "or
2	compromising" after "defeating";
3	(B) in subparagraph (C), by inserting "in-
4	cluding a security vulnerability affecting an in-
5	formation system or a technology included in
6	the critical and emerging technologies list of the
7	Office of Science and Technology Policy or suc-
8	cessor list, such as artificial intelligence (as
9	such term is defined in section 5002 of the Na-
10	tional Artificial Intelligence Initiative Act of
11	2020 (15 U.S.C. 9401)), which may be in a
12	Federal entity's or non-Federal entity's soft-
13	ware or hardware supply chain," after "security
14	vulnerability,";
15	(C) in subparagraph (D), by inserting "or
16	compromise" after "defeat"; and
17	(D) in subparagraph (F), by inserting "or
18	compromised" after "exfiltrated";
19	(2) in paragraph (14), by amending subpara-
20	graph (B) to read as follows:
21	"(B) includes, in accordance with section
22	104(d)(2) of the Cybersecurity Sharing Act of
23	2015 (6 U.S.C. 1503(d)(2))—
24	"(i) operational technology, including
25	industrial control systems, such as super-

1	visory control and data acquisition sys-
2	tems, distributed control systems, and pro-
3	grammable logic controllers;
4	"(ii) edge devices; and
5	"(iii) internet of things devices, in-
6	cluding digital and physical infrastructure
7	impacted by ransomware."; and
8	(3) in paragraph (25), by inserting "or com-
9	promise" after "defeat".

