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:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Widespread Information Management for the Welfare of Infrastructure and Government Act''.

SEC. 2. REAUTHORIZATION OF THE CYBERSECURITY ACT OF 2015.

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

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

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

''(4) ARTIFICIAL INTELLIGENCE.—The term 'artificial intelligence' has the meaning given such term in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401).

''(5) CRITICAL INFRASTRUCTURE.—The term 'critical infrastructure' has the meaning given such term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).''; and

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

''(18) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).'';

(2) in section 103 (6 U.S.C. 1502; relating to sharing of information by the Federal Government)—

(A) in subsection (a), in the matter preceding paragraph (1), by striking ''develop and issue'' and inserting ''develop, issue, and, as appropriate, update''; and

(B) in subsection (b)—

(i) in paragraph (1)—

(I) in the matter preceding subparagraph (A), by inserting ''and, as appropriate, updated,'' after ''developed'';

(II) by amending subparagraph (A) to read as follows:

''(A) ensure the Federal Government maintains the capability to provide technical assistance, on a voluntary basis, to non-Federal entities in utilizing cyber threat indicators and defensive measures for cybersecurity purposes;'';

(III) in subparagraph (E)(ii), by striking ''and'' after the semicolon;

(IV) in subparagraph (F), by striking the period and inserting ''; and''; and

(V) by adding at the end the following new subparagraph:

''(G) pursuant to section 2212 of the Homeland Security Act of 2002 (6 U.S.C. 662), provide one-time read-ins, as appropriate, to select individuals identified by non-Federal entities that own or operate critical infrastructure;''; and

(ii) in paragraph (2)—

(I) by inserting ''and, as appropriate, updating,'' after ''developing''; and

(II) by inserting ''and defensive measures'' after ''promote the sharing of cyber threat indicators''; and

(C) in subsection (e)—

(i) by inserting ''and not later than 60 days after any update, as appropriate, of procedures required by subsection (a),'' after ''Act,''; and

(ii) by inserting ''(or update, as appropriate)'' after ''procedures'';

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

(A) in subsection (c)—

(i) in paragraph (1), by inserting '', including Sector Risk Management Agencies that are agencies and the majority of the systems of which are not covered under subsection (d) or (e) of section 3553 of title 44, United States Code,'' after ''Federal Government''; and

(ii) in paragraph (3)—

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

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

(III) in subparagraph (B), by striking the period and inserting ''; or''; and

(IV) by adding at the end the following 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 ap-

propriate, 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)—

(i) in paragraph (2)(B), by inserting '', and, as appropriate, update,'' after ''review''; and

(ii) in paragraph (3), in the matter preceding subparagraph (A), by inserting ''and, as appropriate, updated,'' after ''required''; and

(C) in subsection (c)—

(i) in paragraph (1)(D), by inserting '', including if such capability and process employs artificial intelligence'' before the semicolon; and

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

''(C) OUTREACH.—Not later than 90 days after the date of the enactment of this subpara-

graph, the Secretary of Homeland Security shall develop and continuously implement an outreach plan, including targeted engagement, to ensure Federal and non-Federal entities, particularly small or rural owners or operators of critical infrastructure which often lack dedicated cybersecurity staff but remain vital to national security—

"(i) are aware of the capability and process required by paragraph (1) to share cyber threat indicators and defensive measures, including the benefits real-time information sharing provides;

"(ii) understand how to share cyber threat indicators and defensive measures;

"(iii) understand the obligation to remove certain personal information in accordance with section 104(d)(7) prior to sharing a cyber threat indicator;

"(iv) understand how cyber threat indicators and defensive measures are received, processed, used, and protected;

"(v) understand the protections they are afforded in sharing any cyber threat indicators and defensive measures; and

"(vi) can provide feedback to the Secretary when policies, procedures, and guidelines that are unclear or unintentionally prohibitive to sharing cyber threat indicators and defensive measures."; and

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

"(D) BRIEFINGS ON OUTREACH.—The Secretary of Homeland Security shall annually provide to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a briefing on the implementation of outreach pursuant to subparagraph (B)."; and

(D) in subsection (d)—

(i) in paragraph (1), by inserting "copyright or" before "trade secret protection"; and

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

(I) in clause (iv), by striking "or" after the semicolon;

(II) in clause (v)(III), by striking the period and inserting "; or"; and

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

"(vi) the purpose of rapidly providing other Federal entities, including Sector Risk Management Agencies, awareness of a cybersecurity threat that may impact the information systems of such Agencies.";

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

(A) in subsection (c)—

(i) in the matter preceding paragraph (1), by striking "shall be" and inserting "may be";

(ii) in paragraph (2), by striking "or" after the semicolon;

(iii) in paragraph (3), by striking the period and inserting "; or"; and

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

"(4) to preclude the use of artificial intelligence that is developed or strictly deployed for cybersecurity purposes in carrying out activities authorized by this title.";

(B) in subsection (f)—

(i) in paragraph (3)—

(I) by inserting ''to share cyber threat indicators or defensive measures'' after ''relationship''; and

(II) by striking ''or'' after the semicolon;

(ii) in paragraph (4), by striking the period and inserting ''; or''; and

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

''(5) to limit or modify, notwithstanding any other provision of law, the authorization to share pursuant to section 104(c)(1) with Sector Risk Management Agencies described in such section.'';

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

(A) in subsection (a)—

(i) by inserting ''and not later than September 30 of every two years thereafter,'' after ''Act,'';

(ii) by inserting ''the Secretary of Homeland Security and'' after ''in coordination with'';

(iii) by inserting ''and the Committee on Homeland Security and Governmental Affairs'' before ''of the Senate'';

(iv) by inserting ''and the Committee on Homeland Security'' before ''of the House''; and

(v) by inserting ''prepositioning activities, ransomware,'' after ''attacks,''; and

(B) in subsection (b)—

(i) in paragraph (1), by inserting ''prepositioning activities, ransomware,'' after ''attacks,'';

(i) in paragraph (2), by inserting ''prepositioning activity, ransomware,'' after ''attack,'';

(i) in paragraph (3), by inserting ''prepositioning activities, ransomware,'' after ''attacks,'' each place it appears; and

(i) in paragraph (4), by inserting ''prepositioning activities, ransomware,'' after ''attacks,''; and

(7) in section 111(a) (6 U.S.C. 1510(a), relating to effective period), by striking ''2025'' and inserting ''2035''.

(b) CONFORMING AMENDMENTS.—Section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650; relating to definitions) is amended—

(1) in paragraph (5)—

(A) in subparagraph (B), by inserting ''or compromising'' after ''defeating'';

(B) in subparagraph (C), by inserting ''including a security vulnerability affecting an information system or a technology included in the critical and emerging technologies list of the Office of Science and Technology Policy or successor list, such as artificial intelligence (as such term is defined in section 5002 of the National Artificial Intelligence Initiative Act of 2020 (15 U.S.C. 9401)), which may be in a Federal entity's or non-Federal entity's software or hardware supply chain,'' after ''security vulnerability,'';

(C) in subparagraph (D), by inserting ''or compromise'' after ''defeat''; and

(D) in subparagraph (F), by inserting ''or compromised'' after ''exfiltrated'';

(2) in paragraph (14), by amending subparagraph (B) to read as follows:

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

''(i) operational technology, including industrial control systems, such as super-

visory control and data acquisition systems, distributed control systems, and programmable logic controllers;

"(ii) edge devices; and

"(iii) internet of things devices, including digital and physical infrastructure impacted by ransomware."; and

(3) in paragraph (25), by inserting "or compromise" after "defeat".

☒