.....

(Original Signature of Member)

119TH CONGRESS
2D SESSION

H. R. _____

To direct the Director of the National Institute of Standards and Technology to establish benchmarks for the timely remediation of software vulnerabilities by owners and operators of critical infrastructure, to establish a grant program for patch modernization and the reduction of the exposure of operational technology, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. WHITESIDES introduced the following bill; which was referred to the Committee on _____

A BILL

To direct the Director of the National Institute of Standards and Technology to establish benchmarks for the timely remediation of software vulnerabilities by owners and operators of critical infrastructure, to establish a grant program for patch modernization and the reduction of the exposure of operational technology, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cyber Resilience for Critical Infrastructure Act''.

SEC. 2. BENCHMARKS AND GRANT PROGRAM RELATED TO ADDRESSING SOFTWARE VULNERABILITIES.

(a) INTERIM CROSS-SECTOR BASELINE.—Not later than 6 months after the date of the enactment of this Act, the Director shall publish an interim cross-sector baseline for critical infrastructure sectors that includes information relating to the following:

(1) Severity tiers for software vulnerabilities, including tiers for vulnerabilities listed in the Known Exploited Vulnerabilities Catalog of the Cybersecurity and Infrastructure Security Agency, critical vulnerabilities, high vulnerabilities, and other vulnerabilities.

(2) Separate tracks for information technology (IT) and operational technology (OT) systems.

(3) Indicators for the following:

(A) The event from which the time to remediate a software vulnerability is measured.

(B) What constitutes elements of remediation with respect to a software vulnerability.

(C) How a compensating control or another form of mitigation, including network segmentation or the elimination of exposure to the

internet, may be utilized if remediation is not available or is impractical due to operational constraints.

(D) How systems for which a vendor has not made available a security update, and end-of-support systems, are treated for purposes of measuring remediation.

(b) BENCHMARKS.—

(1) IN GENERAL.—Not later than 9 months after the date of the enactment of this Act, the Director shall publish benchmarks for the timely remediation of software vulnerabilities by owners and operators of critical infrastructure in the following critical infrastructure sectors:

(A) Communications.

(B) Energy.

(C) Health care and public health.

(D) Water and wastewater systems.

(2) REMAINING BENCHMARKS.—Not later than 15 months after the date of the enactment of this Act, the Director shall publish benchmarks for the timely remediation of software vulnerabilities by owners and operators of critical infrastructure in the following critical infrastructure sectors:

(A) Chemical.

(B) Commercial facilities.

(C) Critical manufacturing.

(D) Dams.

(E) Defense industrial base.

(F) Emergency services.

(G) Financial services.

(H) Food and agriculture.

(I) Government services and facilities.

(J) Information technology.

(K) Nuclear reactors, materials, and waste.

(L) Transportation systems.

(3) GUIDANCE RELATING TO SECTOR CONSTRAINTS.—The Director shall ensure the benchmarks published under paragraphs (1) and (2) provide guidance with respect to any operational constraints that relate to the applicable critical infrastructure sector, including with respect to the following:

(A) Operational tolerance for downtime of operational technology required to remediate a software vulnerability.

(B) Safety risks associated with remediating a software vulnerability in a system that controls a physical process.

(C) Scheduled maintenance windows during which a software vulnerability may be remediated.

(D) Federal or industry certification, approval, or recertification requirements that apply to a system or device before a security update may be deployed (such as requirements for medical devices or aircraft systems).

(E) Vendor release dependencies.

(F) Legacy systems and unsupported systems.

(4) CONSIDERATIONS.—In carrying out paragraphs (1) and (2), the Director shall consider the following:

(A) The 2022 publication by the National Institute of Standards and Technology entitled ''Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology'' (NIST SP 800-40 Rev. 4), or any successor publication.

(B) Control enhancement SI-2(3) of the National Institute of Standards and Technology entitled ''Time to Remediate Flaws and Benchmarks for Corrective Actions'' (published in

NIST SP 800-53 Rev. 5), or any successor control enhancement.

(C) The 2023 special publication by the National Institute of Standards and Technology entitled ''Guide to Operational Technology (OT) Security'' (NIST SP 800-82r3), or any successor special publication.

(5) ADOPTION OF GUIDANCE OR REQUIREMENT.—The Director may carry out paragraphs (1) and (2), by adopting or incorporating by reference, in whole or in part and with such modifications as the Director determines necessary for consistency with the interim cross-sector baseline published under subsection (a), any guidance or requirement related to the applicable critical infrastructure sector, including any of the following:

(A) The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements.

(B) A Transportation Security Administration (TSA) security directive.

(C) A guidance of the Commissioner of Food and Drug Administration relating to postmarket cybersecurity.

(6) NOTIFICATION FOR DELAY.—If the Director does not carry out paragraphs (1) or (2) pursuant to the applicable deadline specified in each such paragraph, respectively, with respect to a critical infrastructure sector, the Director shall carry out the following:

(A) Not later than 30 days after the deadline at issue, submit to the appropriate congressional committees a notice that includes the following:

(i) An explanation for not carrying out the paragraph at issue with respect to the critical infrastructure sector at issue.

(ii) A revised publication date.

(B) Ensure the interim cross-sector baseline published pursuant to subsection (a) applies with respect to the critical infrastructure sector at issue until the Director carries out the paragraph at issue with respect to the critical infrastructure sector at issue.

(7) REVIEWS.—Not later than 3 years after each of the applicable deadlines under paragraphs (1) and (2), respectively, and at least every 3 years thereafter with respect to each such paragraph, the Director shall review any benchmarks published

under each such paragraph, and update such benchmarks as the Director determines necessary.

(c) PUBLIC COMMENT.—Before publishing the interim cross-sector baseline under subsection (a) and the benchmarks under paragraphs (1) and (2) of subsection (b), the Director shall provide a public comment period.

(d) GRANT PROGRAM.—

(1) IN GENERAL.—Not later than 6 months after the later of the date of the enactment of this Act or the date on which amounts are first appropriated pursuant to subsection (f), the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Administrator of the Federal Emergency Management Agency and the heads of the Sector Risk Management Agencies, shall establish a competitive grant program (in this section referred to as the ''program'') to provide grants to eligible entities to carry out a qualifying investment described in paragraph (3) (including any costs related to commercial tool licensing or in-house builds).

(2) AWARDS.—

(A) MULTI-YEAR AWARDS.—The Director of the Cybersecurity and Infrastructure Secu-

rity Agency may provide a grant under the program for a period of more than 1 year.

(B) NO DELAY.—The Director of the Cybersecurity and Infrastructure Security Agency may not delay, withhold, or condition a grant under the program on account of the Director not having published benchmarks under paragraph (1) or (2) of subsection (b) for the critical infrastructure sector of an eligible entity.

(3) QUALIFYING INVESTMENT.—

(A) PATCH MODERNIZATION AND EXPOSURE REDUCTION.—A qualifying investment described in this paragraph may include any of the following:

(i) Adoption of a CI/CD pipeline and automated patch-deployment tooling with respect to software.

(ii) Adoption of staging environments, digital twins, and automated testing infrastructure for validating patches against IT and OT systems before production deployment of software.

(iii) Asset inventory and SBOM ingestion and management tooling with respect to software.

(iv) Application of AI-assisted patch validation and regression-testing tools with respect to software.

(v) Workforce training related to any deployed tooling related to software.

(vi) Network segmentation of operational technology or medical devices from information technology and the internet, including through unidirectional gateways.

(vii) Elimination or hardening of remote access to operational technology.

(viii) Replacement of a network edge device (such as a router, firewall, or virtual private network appliance) that is end-of-support, or that contains a software vulnerability included in the Known Exploited Vulnerabilities Catalog of the Cybersecurity and Infrastructure Security Agency for which the vendor has not made available a security update.

(ix) Any other investment related to the remediation of software vulnerabilities or the reduction of the exposure of operational technology, as determined by the

Director of the Cybersecurity and Infrastructure Security Agency.

(x) Managed services, contracted implementation, or shared regional services to carry out any investment specified in clauses (i) through (ix).

(B) EXCLUSION.—A qualifying investment described in this paragraph does not include any of the following:

(i) General IT modernization not related to—

(I) software patching; or

(II) the reduction of the exposure of operational technology.

(ii) Incident response services related to addressing software vulnerabilities.

(iii) Insurance premiums.

(C) LIMITATION.—A recipient of a grant under the program may apply up to 10 percent of such a grant to qualifying investment specified in subparagraph (A)(v).

(4) APPLICATION.—To apply for a grant under the program, an eligible entity shall submit an application that includes a certification that the eligible entity satisfies, or a 1-year plan with milestones for

the eligible entity to satisfy, with respect to the relevant qualifying investment described in paragraph (3), any of the following:

(A) If no applicable benchmarks are published under paragraph (1) or (2) of subsection (b), as the case may be, as of the application deadline for such grant, the interim cross-sector baseline published under subsection (a).

(B) If the applicable benchmarks are published under paragraph (1) or (2) of subsection (b), as the case may be, as of the application deadline for such grant, such benchmarks.

(5) TIMING.—

(A) UPDATED BENCHMARKS.—

(i) IN GENERAL.—If the Director first publishes, or updates, benchmarks under paragraph (1) or (2) of subsection (b), as the case may be, after the application deadline for a grant received by an eligible entity under the program, such benchmarks may not apply to such entity for the purposes of the plan required under paragraph (4), unless such entity makes a request to the Director of the Cybersecurity

and Infrastructure Security Agency for such benchmarks to apply.

(ii) EXTENSION.—If an eligible entity that receives a grant under the program makes a request under clause (i), the Director of the Cybersecurity and Infrastructure Security Agency shall provide to such entity an extension for such entity to carry out the 1-year plan submitted by such entity under paragraph (4) that allows such entity to carry out such plan beginning on the date on which the Director of Cybersecurity and Infrastructure Security Agency publishes the relevant benchmarks or updated benchmarks.

(B) EXTENSION.—The Director of the Cybersecurity and Infrastructure Security Agency may, as the Director determines appropriate on a case-by-case basis, provide to an eligible entity that receives a grant under the program an extension to carry out the 1-year plan submitted by such entity under paragraph (4) if such plan cannot be carried out in 1 year.

(6) COST SHARE.—

(A) FEDERAL SHARE.—The Director of the Cybersecurity and Infrastructure Security Agency shall ensure, with respect to an eligible entity that receives a grant under the program, the following:

(i) If such entity is a small, rural, or municipal operator or an SLTT entity, such grant is for one hundred percent of the total cost to carry out the 1-year plan submitted by such entity under paragraph (4).

(ii) If such entity is an eligible entity not described in clause (i) or (iii), such grant is for seventy-five percent of the total cost to carry out the plan submitted by such entity under paragraph (4).

(iii) If the entity is a for-profit entity with annual revenue of at least $50,000,000, such grant is for fifty percent of the total cost to carry out the plan submitted by such entity under paragraph (4).

(B) ELIGIBLE ENTITY MATCH.—

(i) IN GENERAL.—An eligible entity specified in clause (ii) or (iii) of subpara-

graph (A) may apply in-kind contributions towards any remaining cost after applying the Federal share specified under such clause, as the case may be, to carry out the plan submitted by such entity under paragraph (4).

(ii) REDUCTION OR WAIVER.—The Director of the Cybersecurity and Infrastructure Security Agency may reduce or waive, with respect to an eligible entity specified in clause (ii) or (iii) of subparagraph (A), the remaining cost after applying the Federal share specified under such clause, as the case may be, to carry out the plan submitted by such entity under paragraph (4), if such entity demonstrates to the Director of the Cybersecurity and Infrastructure Security Agency that such entity has experienced financial hardship, as determined by the Director of the Cybersecurity and Infrastructure Security Agency.

(7) GRANT REPORTING.—

(A) IN GENERAL.—Not later than 1 year after the date on which an eligible entity receives a grant under the program and annually

thereafter, such entity shall submit to the Director of the Cybersecurity and Infrastructure Security Agency a report that uses the measurement definitions of the interim cross-sector baseline published under subsection (a) and includes information relating to the following:

(i) If such entity carries out a qualifying investment described in clauses (i) through (v) of paragraph (3)(A), the mean time for such entity to remediate a software vulnerability included in the Known Exploited Vulnerabilities Catalog of the Cybersecurity and Infrastructure Security Agency.

(ii) Any progress of such entity with respect to the plan submitted by such entity under paragraph (4).

(iii) Any tooling deployed related to software by such entity.

(iv) If such entity carries out an qualifying investment described in clauses (vi) through (viii) of paragraph (3)(A), the number of operational technology assets of such entity that are no longer exposed to

the internet and the number of network edge devices replaced.

(B) PROTECTION.—A report submitted under subparagraph (A) shall be afforded the protections provided under section 2224 of the Homeland Security Act of 2002 (6 U.S.C. 673) for critical infrastructure information voluntarily submitted to the Cybersecurity and Infrastructure Security Agency, and may not be used in any regulatory enforcement action against such entity.

(C) LIMITATION.—The Director of the Cybersecurity and Infrastructure Security Agency may not require a report under subparagraph (A) to identify any specific system, asset, or software vulnerability of such entity.

(8) LIMITED CLAWBACK.—If an eligible entity that receives a grant under the program materially misuses any funds from such a grant, the Director of the Cybersecurity and Infrastructure Security Agency may recoup such funds. The Director of the Cybersecurity and Infrastructure Security Agency may not recoup funds under this paragraph on account of a good faith failure by such entity to satisfy

a milestone in the plan submitted under paragraph (4).

(9) SMALL, RURAL, AND MUNICIPAL OPERATORS.—In carrying out paragraph (1), the Director of the Cybersecurity and Infrastructure Security Agency shall ensure 30 percent of amounts awarded under the program are awarded to eligible entities that are small, rural, or municipal operators, and may provide technical assistance to such entities in lieu of, or in addition to, a grant under the program.

(10) EXCLUSION.—

(A) EXCLUSION.—Except as specified in subparagraph (B), an entity with an annual revenue higher than $10,000,000,000 is not eligible for a grant under this subsection.

(B) EXCEPTION.—The Director of the Cybersecurity and Infrastructure Security Agency may waive the exclusion under subparagraph (A) if the Director of the Cybersecurity and Infrastructure Security Agency determines that providing to an entity specified in such subparagraph a grant under this subsection would address a systemic dependency that affects multiple owners or operators of critical infrastructure or multiple critical infrastructure sectors,

and that the investment funded by such grant would not otherwise be made.

(11) IMPLEMENTATION PRACTICES.—An eligible entity that receives a grant under the program shall ensure that any qualifying investment described in paragraph (3) carried out using such grant, including by a contractor or system integrator, conforms to recognized security practices identified by the Director of the Cybersecurity and Infrastructure Security Agency. With respect to an investment described in paragraph (3)(A)(vi), such entity shall obtain and retain documentation of the resulting network architecture.

(e) REPORT.—Not later than 2 years after the date of the enactment of this Act, the Director and the Director of the Cybersecurity and Infrastructure Security Agency, in coordination with the Comptroller General of the United States, shall jointly submit to the appropriate congressional committees a report that includes information relating to the following:

(1) Any change in the mean time for eligible entities that receive grants under the program to remediate software vulnerabilities included in the Known Exploited Vulnerabilities Catalog of the Cybersecurity and Infrastructure Security Agency since

receiving such grants, compared with sector-wide remediation data available to the Director of the Cybersecurity and Infrastructure Security Agency.

(2) Any change in the exposure of operational technology to the internet with respect to qualifying investments specified in clauses (vi) through (viii) of subsection (d)(3)(A), compared with sector-wide data available to the Director of the Cybersecurity and Infrastructure Security Agency, including through the vulnerability scanning services of the Agency.

(3) Whether the Director satisfied the publication deadlines specified in subsections (a) and (b).

(4) Whether the interim cross-sector baseline was adequate as a basis for the plans required under subsection (d)(4) and the reports required under subsection (d)(7) for critical infrastructure sectors before the publication of the benchmarks under paragraph (1) or (2) of subsection (b), as the case may be.

(5) Any recommendation for additional measures to carry out this section.

(f) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $250,000,000 for fiscal years 2027 through 2031.

(g) RULES OF CONSTRUCTION.—Nothing in this section shall be construed to—

(1) require the Director to carry out rulemaking; or

(2) impose any obligation on any entity, except as a condition of receiving a grant under subsection (d).

(h) DEFINITIONS.—In this section:

(1) ANNUAL REVENUE.—The term ''annual revenue'' means, with respect to an entity, the revenue of such entity for the most recently completed fiscal year before the application deadline for a grant under the program, aggregated with the revenue of any entity that controls, is controlled by, or is under common control with such entity.

(2) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security of the House of Representatives;

(B) the Committee on Science, Space, and Technology of the House of Representatives;

(C) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(D) the Committee on Commerce, Science, and Transportation of the Senate.

(3) 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)).

(4) CRITICAL INFRASTRUCTURE SECTORS.—The term ''critical infrastructure sector'' includes the following sectors:

(A) Chemical.

(B) Commercial facilities.

(C) Communications.

(D) Critical manufacturing.

(E) Dams.

(F) Defense industrial base.

(G) Emergency services.

(H) Energy.

(I) Financial services.

(J) Food and agriculture.

(K) Government services and facilities.

(L) Healthcare and public health.

(M) Information technology.

(N) Nuclear reactors, materials, and waste.

(O) Transportation systems.

(P) Water and wastewater systems.

(5) DIRECTOR.—The term ''Director'' means the Director of the National Institute of Standards and Technology.

(6) ELIGIBLE ENTITY.—The term ''eligible entity'' means any of the following:

(A) An owner or operator of critical infrastructure in any critical infrastructure sector.

(B) A State, local, Tribal, or territorial entity that operates critical infrastructure.

(C) A consortium of eligible entities, each of which is a small, rural, or municipal operator.

(7) OPERATIONAL TECHNOLOGY.—The term ''operational technology'' has the meaning given such term in section 3 of the Internet of Things Cybersecurity Improvement Act of 2020 (15 U.S.C. 278g-3a).

(8) SECTOR RISK MANAGEMENT AGENCY; SLTT ENTITY.—The terms ''Sector Risk Management Agency'' and ''SLTT entity'' have the meanings given such terms in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(9) SMALL, RURAL, OR MUNICIPAL OPERATOR.—The term ''small, rural, or municipal oper-

ator'' means an owner or operator of critical infrastructure that—

(A) serves a population of not more than 10,000, or has fewer than 100 employees (aggregated with any entity that controls, is controlled by, or is under common control with such owner or operator) and annual revenue of less than $50,000,000;

(B) primarily serves a rural area (as defined in section 343(a)(13)(A) of the Consolidated Farm and Rural Development Act (7 U.S.C. 1991(a)(13)(A))); or

(C) is owned or operated by a unit of local government.