.....

(Original Signature of Member)

116TH CONGRESS
2D SESSION

H. R. _____

To amend the Homeland Security Act of 2002 to protect United States critical infrastructure by ensuring that the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security has necessary legal tools to notify entities at risk of cybersecurity vulnerabilities in the enterprise devices or systems that control critical assets of the United States, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

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

A BILL

To amend the Homeland Security Act of 2002 to protect United States critical infrastructure by ensuring that the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security has necessary legal tools to notify entities at risk of cybersecurity vulnerabilities in the enterprise devices or systems that control critical assets of the United States, 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 ''Cybersecurity Vulnerability Identification and Notification Act of 2020''.

SEC. 2. SUBPOENA AUTHORITY.

(a) IN GENERAL.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (a)—

(A) in this subsection, by inserting '', 'cybersecurity purpose','' after '' 'cyber threat indicator' '';

(B) by redesignating paragraphs (3) through (6) as paragraphs (4) through (7), respectively;

(C) by inserting after this subsection the following new paragraph:

''(3) the term 'enterprise device or system'—

''(A) means a device or information system commonly used to perform industrial, commercial, scientific, or governmental functions or processes that relate to critical infrastructure, including operational and industrial control systems, distributed control systems, and programmable logic controllers; and

''(B) does not include personal devices and systems, such as consumer mobile devices, home

computers, residential wireless routers, or residential internet-enabled consumer devices;''.

(D) in paragraph (6), as so redesignated, by striking ''term 'information system' has the meaning given that term in section 3502(8) of title 44; and'' and inserting ''terms 'information system' and 'security vulnerability' have the meanings given those terms in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);'';

(2) in subsection (c)—

(A) in paragraph (8)(C), by striking ''sharing'' and inserting ''share'';

(B) in paragraph (10), by striking ''and'' after the semicolon at the end;

(C) in paragraph (11), by striking the period at the end and inserting ''; and''; and

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

''(12) detecting, identifying, and receiving information about security vulnerabilities relating to information systems for a cybersecurity purpose.''; and

(3) by adding at the end the following new subsection:

''(n) SUBPOENA AUTHORITY.—

''(1) IN GENERAL.—If the Director identifies an information system connected to the internet with a specific security vulnerability and has reason to believe that the security vulnerability relates to critical infrastructure and affects an enterprise device or system of an entity, and the Director made reasonable efforts to identify the entity at risk but was unable to do so, the Director may issue a subpoena for the production of information necessary to identify and notify the entity at risk, in order to carry out a cybersecurity purpose.

''(2) LIMIT ON INFORMATION.—A subpoena issued under this subsection may only seek information in the categories set forth in subparagraphs (A), (B), (D), and (E) of section 2703(c)(2) of title 18, United States Code.

''(3) LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.—The provisions of section 2703(e) of title 18, United States Code, shall apply to any subpoena issued under this subsection.

''(4) COORDINATION.—

''(A) IN GENERAL.—Not later than 60 days after the date of the enactment of this subsection, the Director, in coordination with the Attorney General, shall develop inter-agency

procedures regarding the issuance of subpoenas under this subsection in order to avoid interference with ongoing law enforcement investigations. To the extent practicable, the Director shall coordinate such issuances with the Department of Justice, including the Federal Bureau of Investigation, pursuant to such procedures.

''(B) CONTENTS.—The inter-agency procedures developed under this paragraph shall provide that a subpoena issued by the Director under this subsection shall be—

''(i) issued solely in order to carry out a cybersecurity purpose; and

''(ii) subject to the limitations under this subsection.

''(5) NONCOMPLIANCE.—If any person, partnership, corporation, association, or entity fails to comply with any duly served subpoena issued under this subsection, the Director may request that the Attorney General seek enforcement of the subpoena in any judicial district in which such person, partnership, corporation, association, or entity resides, is found, or transacts business.

''(6) NOTICE.—Not later than seven days after the date on which the Director receives information obtained through a subpoena issued under this subsection, the Director shall notify the entity at risk identified by information obtained under the subpoena regarding the subpoena and the identified security vulnerability.

''(7) AUTHENTICATION.—Any subpoena issued by the Director under this subsection shall be authenticated by the electronic signature of an authorized representative of the Agency or other comparable symbol or process identifying the Agency as the source of the subpoena.

''(8) PROCEDURES.—

''(A) IN GENERAL.—Not later than 90 days after the date of enactment of this subsection, the Director shall establish internal procedures and associated training, applicable to employees and operations of the Agency, regarding subpoenas issued under this subsection, which shall address the following:

''(i) The protection of and restriction on dissemination of nonpublic information obtained through such a subpoena, including a requirement that the Agency may not

disseminate nonpublic information obtained through such a subpoena that identifies the party that is subject to such a subpoena or the entity at risk identified by information obtained as a result of such a subpoena, unless—

''(I) the party or entity consents; or

''(II) the Agency identifies or is notified of a cybersecurity incident involving the party or entity, which relates to the security vulnerability which led to the issuance of such a subpoena.

''(ii) The restriction on the use of information obtained through the subpoena for a cybersecurity purpose.

''(iii) The retention and destruction of nonpublic information obtained through such a subpoena, including the following:

''(I) Immediate destruction of information obtained through such a subpoena that the Director determines is unrelated to critical infrastructure.

''(II) Destruction of any personally identifiable information not later than six months after the date on which the Director receives information obtained through such a subpoena, unless otherwise agreed to by the individual so identified.

''(iv) The process for recordkeeping regarding efforts referred to in paragraph (1) undertaken prior to the issuance of such a subpoena.

''(v) The process for tracking engagement with each party that is subject to such a subpoena and the entity at risk identified by information obtained pursuant to such a subpoena.

''(vi) The process for providing notice to each party that is subject to such a subpoena and each entity at risk identified by information obtained pursuant to such a subpoena.

''(vii) The process and criteria for conducting critical infrastructure security risk assessments to determine whether a

subpoena is necessary prior to being so issued.

''(B) CONGRESSIONAL NOTIFICATION.—The Director shall brief the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate upon establishment of internal procedures and associated training required under this subsection.

''(9) REVIEW OF PROCEDURES.—Not later than one year after the date of enactment of this subsection, the Privacy Officer of the Agency, in consultation with the Privacy Officer of the Department, shall—

''(A) review the internal procedures and associated training established by the Director under paragraph (8) to ensure that—

''(i) the procedures and training are consistent with fair information practices; and

''(ii) the operations of the Agency comply with the procedures and training; and

''(B) notify the Committee on Homeland Security of the House of Representatives and

the Committee on Homeland Security and Governmental Affairs of the Senate of the results of such review.

''(10) RESOURCE ASSESSMENT.—Not later than 120 days after the date of the enactment of this subsection, the Director shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate an assessment regarding whether additional resources are required to—

''(A)(i) ensure timely notifications to entities at risk pursuant to paragraph (6); and

''(ii) provide such entities at risk with timely support to mitigate security vulnerabilities; and

''(B) provide associated training applicable to employees and operations of the Agency to comply with internal procedures established pursuant to paragraph (8).

''(11) PUBLICATION OF INFORMATION.—Not later than 120 days after establishing the internal procedures and policies under paragraph (8), the Director shall make publicly available, including on a Department website, information regarding the sub-

poena process under this subsection, including regarding the following:

''(A) The purpose for subpoenas issued under this subsection.

''(B) The subpoena process.

''(C) The criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena.

''(D) Policies and procedures on retention and sharing of data obtained by subpoena.

''(E) The process for providing notice to each entity at risk identified by information obtained pursuant to a subpoena issued under this subsection, and contact information that such an entity may use to confirm the authenticity of such notice.

''(F) Guidelines on how entities at risk contacted by the Director may respond to notice of a subpoena.

''(G) The internal procedures of the Agency established pursuant to paragraph (8).

''(12) ANNUAL REPORTS.—Not later than six months after the establishment of the internal procedures and associated training pursuant to paragraph (8) and annually thereafter, the Director shall sub-

mit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report (which may include a classified annex but with the presumption of declassification) on the use of subpoenas under this subsection by the Director, which shall include the following:

''(A) A discussion of the following:

''(i) The effectiveness of the use of subpoenas to mitigate security vulnerabilities.

''(ii) The critical infrastructure security risk assessment process conducted for subpoenas issued under this subsection.

''(iii) The number of subpoenas issued under this subsection by the Director during the preceding year.

''(iv) To the extent practicable, the number of vulnerable enterprise devices or systems mitigated under this subsection by the Agency during the preceding year.

''(v) The number of entities notified by the Director under this subsection, and their responses, during the preceding year.

''(B) For each subpoena issued under this subsection, the following:

''(i) The source of the security vulnerability at issue detected, identified, or received by the Director.

''(ii) A description of the efforts undertaken to identify the entity at risk prior to issuing each such subpoena.

''(iii) A description of the outcome of each such subpoena, including discussion regarding the resolution or mitigation of the security vulnerability at issue.

''(iv) A description of any additional support provided by the Director to the entity at risk.

''(13) PUBLICATION OF THE ANNUAL REPORTS.—The Director shall make publicly available a version of each annual report required under paragraph (12), which shall at a minimum include the findings described in clause (iii), (iv), and (v) of this subsection of such paragraph.

''(14) DHS INSPECTOR GENERAL REPORT.—Not later than one year after the date of the enactment of this subsection, the Inspector General of the Department shall submit to the Committee on

Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report evaluating the Agency's compliance with the following:

"(A) The inter-agency procedures established under paragraph (4).

"(B) The internal procedures and associated training established pursuant to paragraph (8).".