

.....
(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.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Cybersecurity Vulner-
3 ability Identification and Notification Act of 2019”.

4 **SEC. 2. SUBPOENA AUTHORITY.**

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

7 (1) in subsection (a)—

8 (A) in this subsection, by inserting “, ‘cy-
9 bersecurity purpose,’” after “‘cyber threat indi-
10 cator’”;

11 (B) by redesignating paragraphs (3)
12 through (6) as paragraphs (4) through (7), re-
13 spectively;

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

16 “(3) the term ‘enterprise device or system’—

17 “(A) means a device or information system
18 commonly used to perform industrial, commer-
19 cial, scientific, or governmental functions or
20 processes that relate to critical infrastructure,
21 including operational and industrial control sys-
22 tems, distributed control systems, and program-
23 mable logic controllers; and

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

1 computers, residential wireless routers, or resi-
2 dential internet-enabled consumer devices;”.

3 (D) in paragraph (6), as so redesignated,
4 by striking “term ‘information system’ has the
5 meaning given that term in section 3502(8) of
6 title 44; and” and inserting “terms ‘information
7 system’ and ‘security vulnerability’ have the
8 meanings given those terms in section 102 of
9 the Cybersecurity Information Sharing Act of
10 2015 (6 U.S.C. 1501);”;

11 (2) in subsection (c)—

12 (A) in paragraph (8)(C), by striking “shar-
13 ing” and inserting “share”;

14 (B) in paragraph (10), by striking “and”
15 after the semicolon at the end;

16 (C) in paragraph (11), by striking the pe-
17 riod at the end and inserting “; and”; and

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

20 “(12) detecting, identifying, and receiving infor-
21 mation about security vulnerabilities relating to in-
22 formation systems for a cybersecurity purpose.”; and

23 (3) by adding at the end the following new sub-
24 section:

25 “(n) SUBPOENA AUTHORITY.—

1 “(1) IN GENERAL.—If the Director identifies an
2 information system connected to the internet with a
3 specific security vulnerability and has reason to be-
4 lieve that the security vulnerability relates to critical
5 infrastructure and affects an enterprise device or
6 system of an entity, and the Director made reason-
7 able efforts to identify the entity at risk but was un-
8 able to do so, the Director may issue a subpoena for
9 the production of information necessary to identify
10 and notify the entity at risk, in order to carry out
11 a cybersecurity purpose.

12 “(2) LIMIT ON INFORMATION.—A subpoena
13 issued under this subsection may only seek informa-
14 tion in the categories set forth in subparagraphs
15 (A), (B), (D), and (E) of section 2703(c)(2) of title
16 18, United States Code.

17 “(3) LIABILITY PROTECTIONS FOR DISCLOSING
18 PROVIDERS.—The provisions of section 2703(e) of
19 title 18, United States Code, shall apply to any sub-
20 poena issued under this subsection.

21 “(4) COORDINATION.—

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

1 procedures regarding the issuance of subpoenas
2 under this subsection in order to avoid inter-
3 ference with ongoing law enforcement investiga-
4 tions. To the extent practicable, the Director
5 shall coordinate such issuances with the De-
6 partment of Justice, including the Federal Bu-
7 reau of Investigation, pursuant to such proce-
8 dures.

9 “(B) CONTENTS.—The inter-agency proce-
10 dures developed under this paragraph shall pro-
11 vide that a subpoena issued by the Director
12 under this subsection shall be—

13 “(i) issued solely in order to carry out
14 a cybersecurity purpose; and

15 “(ii) subject to the limitations under
16 this subsection.

17 “(5) NONCOMPLIANCE.—If any person, part-
18 nership, corporation, association, or entity fails to
19 comply with any duly served subpoena issued under
20 this subsection, the Director may request that the
21 Attorney General seek enforcement of the subpoena
22 in any judicial district in which such person, part-
23 nership, corporation, association, or entity resides, is
24 found, or transacts business.

1 “(6) NOTICE.—Not later than seven days after
2 the date on which the Director receives information
3 obtained through a subpoena issued under this sub-
4 section, the Director shall notify the entity at risk
5 identified by information obtained under the sub-
6 poena regarding the subpoena and the identified se-
7 curity vulnerability.

8 “(7) AUTHENTICATION.—Any subpoena issued
9 by the Director under this subsection shall be au-
10 thenticated by the electronic signature of an author-
11 ized representative of the Agency or other com-
12 parable symbol or process identifying the Agency as
13 the source of the subpoena.

14 “(8) PROCEDURES.—

15 “(A) IN GENERAL.—Not later than 90
16 days after the date of enactment of this sub-
17 section, the Director shall establish internal
18 procedures and associated training, applicable
19 to employees and operations of the Agency, re-
20 garding subpoenas issued under this subsection,
21 which shall address the following:

22 “(i) The protection of and restriction
23 on dissemination of nonpublic information
24 obtained through such a subpoena, includ-
25 ing a requirement that the Agency may not

1 disseminate nonpublic information ob-
2 tained through such a subpoena that iden-
3 tifies the party that is subject to such a
4 subpoena or the entity at risk identified by
5 information obtained as a result of such a
6 subpoena, unless—

7 “(I) the party or entity consents;

8 or

9 “(II) the Agency identifies or is
10 notified of a cybersecurity incident in-
11 volving the party or entity, which re-
12 lates to the security vulnerability
13 which led to the issuance of such a
14 subpoena.

15 “(ii) The restriction on the use of in-
16 formation obtained through the subpoena
17 for a cybersecurity purpose.

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

21 “(I) Immediate destruction of in-
22 formation obtained through such a
23 subpoena that the Director determines
24 is unrelated to critical infrastructure.

1 “(II) Destruction of any person-
2 ally identifiable information not later
3 than six months after the date on
4 which the Director receives informa-
5 tion obtained through such a sub-
6 poena, unless otherwise agreed to by
7 the individual so identified.

8 “(iv) The process for recordkeeping
9 regarding efforts referred to in paragraph
10 (1) undertaken prior to the issuance of
11 such a subpoena.

12 “(v) The process for tracking engage-
13 ment with each party that is subject to
14 such a subpoena and the entity at risk
15 identified by information obtained pursu-
16 ant to such a subpoena.

17 “(vi) The process for providing notice
18 to each party that is subject to such a sub-
19 poena and each entity at risk identified by
20 information obtained pursuant to such a
21 subpoena.

22 “(vii) The process and criteria for
23 conducting critical infrastructure security
24 risk assessments to determine whether a

1 subpoena is necessary prior to being so
2 issued.

3 “(B) CONGRESSIONAL NOTIFICATION.—
4 The Director shall brief the Committee on
5 Homeland Security of the House of Representa-
6 tives and the Committee on Homeland Security
7 and Governmental Affairs of the Senate upon
8 establishment of internal procedures and associ-
9 ated training required under this subsection.

10 “(9) REVIEW OF PROCEDURES.—Not later than
11 one year after the date of enactment of this sub-
12 section, the Privacy Officer of the Agency, in con-
13 sultation with the Privacy Officer of the Depart-
14 ment, shall—

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

18 “(i) the procedures and training are
19 consistent with fair information practices;
20 and

21 “(ii) the operations of the Agency
22 comply with the procedures and training;
23 and

24 “(B) notify the Committee on Homeland
25 Security of the House of Representatives and

1 the Committee on Homeland Security and Gov-
2 ernmental Affairs of the Senate of the results
3 of such review.

4 “(10) RESOURCE ASSESSMENT.—Not later than
5 120 days after the date of the enactment of this
6 subsection, the Director shall submit to the Com-
7 mittee on Homeland Security of the House of Rep-
8 resentatives and the Committee on Homeland Secu-
9 rity and Governmental Affairs of the Senate an as-
10 sessment regarding whether additional resources are
11 required to—

12 “(A)(i) ensure timely notifications to enti-
13 ties at risk pursuant to paragraph (6); and

14 “(ii) provide such entities at risk with
15 timely support to mitigate security
16 vulnerabilities; and

17 “(B) provide associated training applicable
18 to employees and operations of the Agency to
19 comply with internal procedures established
20 pursuant to paragraph (8).

21 “(11) PUBLICATION OF INFORMATION.—Not
22 later than 120 days after establishing the internal
23 procedures and policies under paragraph (8), the Di-
24 rector shall make publicly available, including on a
25 Department website, information regarding the sub-

1 poena process under this subsection, including re-
2 garding the following:

3 “(A) The purpose for subpoenas issued
4 under this subsection.

5 “(B) The subpoena process.

6 “(C) The criteria for the critical infra-
7 structure security risk assessment conducted
8 prior to issuing a subpoena.

9 “(D) Policies and procedures on retention
10 and sharing of data obtained by subpoena.

11 “(E) The process for providing notice to
12 each entity at risk identified by information ob-
13 tained pursuant to a subpoena issued under
14 this subsection, and contact information that
15 such an entity may use to confirm the authen-
16 ticity of such notice.

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

20 “(G) The internal procedures of the Agen-
21 cy established pursuant to paragraph (8).

22 “(12) ANNUAL REPORTS.—Not later than six
23 months after the establishment of the internal proce-
24 dures and associated training pursuant to paragraph
25 (8) and annually thereafter, the Director shall sub-

1 mit to the Committee on Homeland Security and
2 Governmental Affairs of the Senate and the Com-
3 mittee on Homeland Security of the House of Rep-
4 resentatives a report (which may include a classified
5 annex but with the presumption of declassification)
6 on the use of subpoenas under this subsection by the
7 Director, which shall include the following:

8 “(A) A discussion of the following:

9 “(i) The effectiveness of the use of
10 subpoenas to mitigate security
11 vulnerabilities.

12 “(ii) The critical infrastructure secu-
13 rity risk assessment process conducted for
14 subpoenas issued under this subsection.

15 “(iii) The number of subpoenas issued
16 under this subsection by the Director dur-
17 ing the preceding year.

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

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

1 “(B) For each subpoena issued under this
2 subsection, the following:

3 “(i) The source of the security vulner-
4 ability at issue detected, identified, or re-
5 ceived by the Director.

6 “(ii) A description of the efforts un-
7 dertaken to identify the entity at risk prior
8 to issuing each such subpoena.

9 “(iii) A description of the outcome of
10 each such subpoena, including discussion
11 regarding the resolution or mitigation of
12 the security vulnerability at issue.

13 “(iv) A description of any additional
14 support provided by the Director to the en-
15 tity at risk.

16 “(13) PUBLICATION OF THE ANNUAL RE-
17 PORTS.—The Director shall make publicly available
18 a version of each annual report required under para-
19 graph (12), which shall at a minimum include the
20 findings described in clause (iii), (iv), and (v) of this
21 subsection of such paragraph.

22 “(14) DHS INSPECTOR GENERAL REPORT.—
23 Not later than one year after the date of the enact-
24 ment of this subsection, the Inspector General of the
25 Department shall submit to the Committee on

1 Homeland Security of the House of Representatives
2 and the Committee on Homeland Security and Gov-
3 ernmental Affairs of the Senate a report evaluating
4 the Agency's compliance with the following:

5 “(A) The inter-agency procedures estab-
6 lished under paragraph (4).

7 “(B) The internal procedures and associ-
8 ated training established pursuant to paragraph
9 (8).”.