

116TH CONGRESS
1ST SESSION

S. 3045

To amend the Homeland Security Act of 2002 to protect United States critical infrastructure by ensuring that the Cybersecurity and Infrastructure Security Agency has the legal tools it needs to notify private and public sector entities put at risk by cybersecurity vulnerabilities in the networks and systems that control critical assets of the United States.

IN THE SENATE OF THE UNITED STATES

DECEMBER 12, 2019

Mr. JOHNSON (for himself and Ms. HASSAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

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 has the legal tools it needs to notify private and public sector entities put at risk by cybersecurity vulnerabilities in the networks and systems that control critical assets of the United States.

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) by redesignating paragraph (6) as
9 paragraph (7); and

10 (B) by inserting after paragraph (5) the
11 following:

12 “(6) the term ‘security vulnerability’ has the
13 meaning given that term in section 102(17) of the
14 Cybersecurity Information Sharing Act of 2015 (6
15 U.S.C. 1501(17));”;

16 (2) in subsection (c)—

17 (A) in paragraph (10), by striking “and”
18 at the end;

19 (B) in paragraph (11), by striking the pe-
20 riod at the end and inserting “; and”; and

21 (C) by adding at the end the following:

22 “(12) detecting, identifying, and receiving infor-
23 mation about security vulnerabilities relating to crit-
24 ical infrastructure in the information systems and
25 devices of Federal and non-Federal entities for a cy-
26 bersecurity purpose, as defined in section 102 of the

1 Cybersecurity Information Sharing Act of 2015 (6
2 U.S.C. 1501).”; and

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

4 “(n) SUBPOENA AUTHORITY.—

5 “(1) DEFINITION.—In this subsection, the term
6 ‘enterprise device or system’—

7 “(A) means a device or system commonly
8 used to perform industrial, commercial, sci-
9 entific, or governmental functions or processes
10 that relate to critical infrastructure, including
11 operational and industrial control systems, dis-
12 tributed control systems, and programmable
13 logic controllers; and

14 “(B) does not include personal devices and
15 systems, such as consumer mobile devices, home
16 computers, residential wireless routers, or resi-
17 dential internet-enabled consumer devices.

18 “(2) AUTHORITY.—

19 “(A) IN GENERAL.—If the Director identi-
20 fies a system connected to the internet with a
21 specific security vulnerability and has reason to
22 believe that the security vulnerability relates to
23 critical infrastructure and affects an enterprise
24 device or system owned or operated by a Fed-
25 eral or non-Federal entity, and the Director is

1 unable to identify the entity at risk, the Direc-
2 tor may issue a subpoena for the production of
3 information necessary to identify and notify the
4 entity at risk, in order to carry out a function
5 authorized under subsection (c)(12).

6 “(B) LIMIT ON INFORMATION.—A sub-
7 poena issued under the authority under sub-
8 paragraph (A) may only seek information in the
9 categories set forth in subparagraphs (A), (B),
10 (D), and (E) of section 2703(c)(2) of title 18,
11 United States Code.

12 “(C) LIABILITY PROTECTIONS FOR DIS-
13 CLOSING PROVIDERS.—The provisions of section
14 2703(e) of title 18, United States Code, shall
15 apply to any subpoena issued under the author-
16 ity under subparagraph (A).

17 “(3) COORDINATION.—

18 “(A) IN GENERAL.—If the Director decides
19 to exercise the subpoena authority under this
20 subsection, and in the interest of avoiding inter-
21 ference with ongoing law enforcement investiga-
22 tions, the Director shall coordinate the issuance
23 of any such subpoena with the Department of
24 Justice, including the Federal Bureau of Inves-
25 tigation, pursuant to inter-agency procedures

1 which the Director, in coordination with the At-
2 torney General, shall develop not later than 60
3 days after the date of enactment of this sub-
4 section.

5 “(B) CONTENTS.—The inter-agency proce-
6 dures developed under this paragraph shall pro-
7 vide that a subpoena issued by the Director
8 under this subsection shall be—

9 “(i) issued in order to carry out a
10 function described in subsection (c)(12);
11 and

12 “(ii) subject to the limitations under
13 this subsection.

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

22 “(5) NOTICE.—Not later than 7 days after the
23 date on which the Director receives information ob-
24 tained through a subpoena issued under this sub-
25 section, the Director shall notify the entity at risk

1 identified by information obtained under the sub-
2 poena regarding the subpoena and the identified vul-
3 nerability.

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

10 “(7) PROCEDURES.—Not later than 90 days
11 after the date of enactment of this subsection, the
12 Director shall establish internal procedures and as-
13 sociated training, applicable to employees and oper-
14 ations of the Agency, regarding subpoenas issued
15 under this subsection, which shall address—

16 “(A) the protection of and restriction on
17 dissemination of nonpublic information obtained
18 through a subpoena issued under this sub-
19 section, including a requirement that the Agen-
20 cy shall not disseminate nonpublic information
21 obtained through a subpoena issued under this
22 subsection that identifies the party that is sub-
23 ject to the subpoena or the entity at risk identi-
24 fied by information obtained, unless—

25 “(i) the party or entity consents; or

1 “(ii) the Agency identifies or is noti-
2 fied of a cybersecurity incident involving
3 the party or entity, which relates to the
4 vulnerability which led to the issuance of
5 the subpoena;

6 “(B) the restriction on the use of informa-
7 tion obtained through the subpoena for a cyber-
8 security purpose, as defined in section 102 of
9 the Cybersecurity Information Sharing Act of
10 2015 (6 U.S.C. 1501);

11 “(C) the retention and destruction of non-
12 public information obtained through a subpoena
13 issued under this subsection, including—

14 “(i) immediate destruction of informa-
15 tion obtained through the subpoena that
16 the Director determines is unrelated to
17 critical infrastructure; and

18 “(ii) destruction of any personally
19 identifiable information not later than 6
20 months after the date on which the Direc-
21 tor receives information obtained through
22 the subpoena, unless otherwise agreed to
23 by the individual identified by the sub-
24 poena respondent;

1 “(D) the processes for providing notice to
2 each party that is subject to the subpoena and
3 each entity at risk identified by information ob-
4 tained pursuant to a subpoena issued under
5 this subsection; and

6 “(E) the processes and criteria for con-
7 ducting critical infrastructure security risk as-
8 sessments to determine whether a subpoena is
9 necessary prior to being issued under this sub-
10 section.

11 “(8) REVIEW OF PROCEDURES.—Not later than
12 1 year after the date of enactment of this sub-
13 section, the Privacy Officer of the Agency shall—

14 “(A) review the procedures developed by
15 the Director under paragraph (7) to ensure
16 that—

17 “(i) the procedures are consistent with
18 fair information practices; and

19 “(ii) the operations of the Agency
20 comply with the procedures; and

21 “(B) notify the Committee on Homeland
22 Security and Governmental Affairs of the Sen-
23 ate and the Committee on Homeland Security
24 of the House of Representatives of the results
25 of the review.

1 “(9) PUBLICATION OF INFORMATION.—Not
2 later than 120 days after establishing the internal
3 procedures under paragraph (7), the Director shall
4 make publicly available information regarding the
5 subpoena process under this subsection, including
6 regarding—

7 “(A) the purpose for subpoenas issued
8 under this subsection;

9 “(B) the subpoena process;

10 “(C) the criteria for the critical infrastruc-
11 ture security risk assessment conducted prior to
12 issuing a subpoena;

13 “(D) policies and procedures on retention
14 and sharing of data obtained by subpoena;

15 “(E) guidelines on how entities contacted
16 by the Director may respond to notice of a sub-
17 poena; and

18 “(F) the procedures and policies of the
19 Agency developed under paragraph (7).

20 “(10) ANNUAL REPORTS.—The Director shall
21 annually submit to the Committee on Homeland Se-
22 curity and Governmental Affairs of the Senate and
23 the Committee on Homeland Security of the House
24 of Representatives a report (which may include a
25 classified annex but with the presumption of declas-

1 sification) on the use of subpoenas under this sub-
2 section by the Director, which shall include—

3 “(A) a discussion of—

4 “(i) the effectiveness of the use of
5 subpoenas to mitigate critical infrastruc-
6 ture security vulnerabilities;

7 “(ii) the critical infrastructure secu-
8 rity risk assessment process conducted for
9 subpoenas issued under this subsection;

10 “(iii) the number of subpoenas issued
11 under this subsection by the Director dur-
12 ing the preceding year;

13 “(iv) to the extent practicable, the
14 number of vulnerable enterprise devices or
15 systems mitigated under this subsection by
16 the Agency during the preceding year; and

17 “(v) the number of entities notified by
18 the Director under this subsection, and
19 their response, during the previous year;
20 and

21 “(B) for each subpoena issued under this
22 subsection—

23 “(i) the source of the security vulner-
24 ability detected, identified, or received by
25 the Director;

1 “(ii) the steps taken to identify the
2 entity at risk prior to issuing the sub-
3 poena; and

4 “(iii) a description of the outcome of
5 the subpoena, including discussion on the
6 resolution or mitigation of the critical in-
7 frastructure security vulnerability.

8 “(11) PUBLICATION OF THE ANNUAL RE-
9 PORTS.—The Director shall make a version of the
10 annual report required by paragraph (10) publicly
11 available, which shall, at a minimum, include the
12 findings described in clause (iii), (iv) and (v) of sub-
13 paragraph (A).”.

○