

Calendar No. 500116TH CONGRESS
2^D SESSION**S. 3045****[Report No. 116-242]**

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, Ms. HASSAN, Mr. WYDEN, and Mr. KING) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

JULY 29, 2020

Reported by Mr. JOHNSON, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italic*]

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,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cybersecurity Vulner-

5 ability Identification and Notification Act of 2019”.

6 **SEC. 2. SUBPOENA AUTHORITY.**

7 (a) **IN GENERAL.**—Section 2209 of the Homeland

8 Security Act of 2002 (6 U.S.C. 659) is amended—

9 (1) in subsection (a)—

10 (A) by redesignating paragraph (6) as

11 paragraph (7); and

12 (B) by inserting after paragraph (5) the

13 following:

14 “(6) the term ‘security vulnerability’ has the

15 meaning given that term in section 102(17) of the

16 Cybersecurity Information Sharing Act of 2015 (6

17 U.S.C. 1501(17));”;

18 (2) in subsection (c)—

19 (A) in paragraph (10), by striking “and”

20 at the end;

21 (B) in paragraph (11), by striking the pe-

22 riod at the end and inserting “; and”;

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

24 “(12) detecting, identifying, and receiving infor-

25 mation about security vulnerabilities relating to crit-

1 ical infrastructure in the information systems and
 2 devices of Federal and non-Federal entities for a cy-
 3 bersecurity purpose, as defined in section 102 of the
 4 Cybersecurity Information Sharing Act of 2015 (6
 5 U.S.C. 1501).”;

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

7 “(n) SUBPOENA AUTHORITY.—

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

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

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

21 “(2) AUTHORITY.—

22 “(A) IN GENERAL.—If the Director identi-
 23 fies a system connected to the internet with a
 24 specific security vulnerability and has reason to
 25 believe that the security vulnerability relates to

1 critical infrastructure and affects an enterprise
2 device or system owned or operated by a Fed-
3 eral or non-Federal entity, and the Director is
4 unable to identify the entity at risk, the Direc-
5 tor may issue a subpoena for the production of
6 information necessary to identify and notify the
7 entity at risk, in order to carry out a function
8 authorized under subsection (e)(12).

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

15 “(C) LIABILITY PROTECTIONS FOR DIS-
16 CLOSING PROVIDERS.—The provisions of section
17 2703(e) of title 18, United States Code, shall
18 apply to any subpoena issued under the author-
19 ity under subparagraph (A).

20 “(3) COORDINATION.—

21 “(A) IN GENERAL.—If the Director decides
22 to exercise the subpoena authority under this
23 subsection, and in the interest of avoiding inter-
24 ference with ongoing law enforcement investiga-
25 tions, the Director shall coordinate the issuance

1 of any such subpoena with the Department of
2 Justice, including the Federal Bureau of Inves-
3 tigation, pursuant to inter-agency procedures
4 which the Director, in coordination with the At-
5 torney General, shall develop not later than 60
6 days after the date of enactment of this sub-
7 section.

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

12 “(i) issued in order to carry out a
13 function described in subsection (c)(12);
14 and

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

17 “(4) 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 “(5) NOTICE.—Not later than 7 days after the
2 date on which the Director receives information ob-
3 tained 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 vul-
7 nerability.

8 “(6) 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 “(7) PROCEDURES.—Not later than 90 days
15 after the date of enactment of this subsection, the
16 Director shall establish internal procedures and as-
17 sociated training, applicable to employees and oper-
18 ations of the Agency, regarding subpoenas issued
19 under this subsection, which shall address—

20 “(A) the protection of and restriction on
21 dissemination of nonpublic information obtained
22 through a subpoena issued under this sub-
23 section, including a requirement that the Agen-
24 cy shall not disseminate nonpublic information
25 obtained through a subpoena issued under this

1 subsection that identifies the party that is sub-
2 ject to the subpoena or the entity at risk identi-
3 fied by information obtained, unless—

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

5 “(ii) the Agency identifies or is noti-
6 fied of a cybersecurity incident involving
7 the party or entity, which relates to the
8 vulnerability which led to the issuance of
9 the subpoena;

10 “(B) the restriction on the use of informa-
11 tion obtained through the subpoena for a cyber-
12 security purpose, as defined in section 102 of
13 the Cybersecurity Information Sharing Act of
14 2015 (6 U.S.C. 1501);

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

18 “(i) immediate destruction of informa-
19 tion obtained through the subpoena that
20 the Director determines is unrelated to
21 critical infrastructure; and

22 “(ii) destruction of any personally
23 identifiable information not later than 6
24 months after the date on which the Direc-
25 tor receives information obtained through

1 the subpoena, unless otherwise agreed to
2 by the individual identified by the sub-
3 poena respondent;

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

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

14 “(8) REVIEW OF PROCEDURES.—Not later than
15 1 year after the date of enactment of this sub-
16 section, the Privacy Officer of the Agency shall—

17 “(A) review the procedures developed by
18 the Director under paragraph (7) to ensure
19 that—

20 “(i) the procedures are consistent with
21 fair information practices; and

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

24 “(B) notify the Committee on Homeland
25 Security and Governmental Affairs of the Sen-

1 ate and the Committee on Homeland Security
2 of the House of Representatives of the results
3 of the review.

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

10 “(A) the purpose for subpoenas issued
11 under this subsection;

12 “(B) the subpoena process;

13 “(C) the criteria for the critical infrastruc-
14 ture security risk assessment conducted prior to
15 issuing a subpoena;

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

18 “(E) guidelines on how entities contacted
19 by the Director may respond to notice of a sub-
20 poena; and

21 “(F) the procedures and policies of the
22 Agency developed under paragraph (7).

23 “(10) ANNUAL REPORTS.—The Director shall
24 annually submit to the Committee on Homeland Se-
25 curity and Governmental Affairs of the Senate and

1 the Committee on Homeland Security of the House
2 of Representatives a report (which may include a
3 classified annex but with the presumption of declas-
4 sification) on the use of subpoenas under this sub-
5 section by the Director, which shall include—

6 “(A) a discussion of—

7 “(i) the effectiveness of the use of
8 subpoenas to mitigate critical infrastruc-
9 ture security vulnerabilities;

10 “(ii) the critical infrastructure secu-
11 rity risk assessment process conducted for
12 subpoenas issued under this subsection;

13 “(iii) the number of subpoenas issued
14 under this subsection by the Director dur-
15 ing the preceding year;

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

20 “(v) the number of entities notified by
21 the Director under this subsection; and
22 their response; during the previous year;
23 and

24 “(B) for each subpoena issued under this
25 subsection—

1 “(i) the source of the security vulner-
2 ability detected, identified, or received by
3 the Director;

4 “(ii) the steps taken to identify the
5 entity at risk prior to issuing the sub-
6 poena; and

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

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

17 **SECTION 1. SHORT TITLE.**

18 *This Act may be cited as the “Cybersecurity Vulner-*
19 *ability Identification and Notification Act of 2020”.*

20 **SEC. 2. SUBPOENA AUTHORITY.**

21 *(a) IN GENERAL.—Section 2209 of the Homeland Se-*
22 *curity Act of 2002 (6 U.S.C. 659) is amended—*

23 *(1) in subsection (a)—*

24 *(A) in paragraph (5), by striking “and” at*
25 *the end;*

1 (B) by redesignating paragraph (6) as
2 paragraph (7); and

3 (C) by inserting after paragraph (5) the fol-
4 lowing:

5 “(6) the term ‘security vulnerability’ has the
6 meaning given that term in section 102(17) of the Cy-
7 bersecurity Information Sharing Act of 2015 (6
8 U.S.C. 1501(17)); and”;

9 (2) in subsection (c)—

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

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

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

15 “(12) detecting, identifying, and receiving infor-
16 mation about security vulnerabilities relating to crit-
17 ical infrastructure in the information systems and de-
18 vices of Federal and non-Federal entities for a cyber-
19 security purpose, as defined in section 102 of the Cy-
20 bersecurity Information Sharing Act of 2015 (6
21 U.S.C. 1501).”; and

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

23 “(o) SUBPOENA AUTHORITY.—

24 “(1) DEFINITION.—In this subsection, the term
25 ‘covered device or system’—

1 “(A) means a device or system commonly
2 used to perform industrial, commercial, sci-
3 entific, or governmental functions or processes
4 that relate to critical infrastructure, including
5 operational and industrial control systems, dis-
6 tributed control systems, and programmable logic
7 controllers; and

8 “(B) does not include personal devices and
9 systems, such as consumer mobile devices, home
10 computers, residential wireless routers, or resi-
11 dential internet enabled consumer devices.

12 “(2) AUTHORITY.—

13 “(A) IN GENERAL.—If the Director identi-
14 fies a system connected to the internet with a
15 specific security vulnerability and has reason to
16 believe that the security vulnerability relates to
17 critical infrastructure and affects a covered de-
18 vice or system owned or operated by a Federal
19 or non-Federal entity, and the Director is unable
20 to identify the entity at risk, the Director may
21 issue a subpoena for the production of informa-
22 tion necessary to identify and notify the entity
23 at risk, in order to carry out a function author-
24 ized under subsection (c)(12).

1 “(B) *LIMIT ON INFORMATION.*—A subpoena
2 issued under the authority under subparagraph
3 (A) may seek information—

4 “(i) *only in the categories set forth in*
5 *subparagraphs (A), (B), (D), and (E) of*
6 *section 2703(c)(2) of title 18, United States*
7 *Code; and*

8 “(ii) *for not more than 20 covered de-*
9 *vices or systems.*

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

15 “(3) *COORDINATION.*—

16 “(A) *IN GENERAL.*—If the Director decides
17 to exercise the subpoena authority under this
18 subsection, and in the interest of avoiding inter-
19 ference with ongoing law enforcement investiga-
20 tions, the Director shall coordinate the issuance
21 of any such subpoena with the Department of
22 Justice, including the Federal Bureau of Inves-
23 tigation, pursuant to inter-agency procedures
24 which the Director, in coordination with the At-
25 torney General, shall develop not later than 60

1 *days after the date of enactment of this sub-*
2 *section.*

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

7 “(i) *issued in order to carry out a*
8 *function described in subsection (c)(12); and*

9 “(ii) *subject to the limitations under*
10 *this subsection.*

11 “(4) *NONCOMPLIANCE.—If any person, partner-*
12 *ship, corporation, association, or entity fails to com-*
13 *ply with any duly served subpoena issued under this*
14 *subsection, the Director may request that the Attorney*
15 *General seek enforcement of the subpoena in any judi-*
16 *cial district in which such person, partnership, cor-*
17 *poration, association, or entity resides, is found, or*
18 *transacts business.*

19 “(5) *NOTICE.—Not later than 7 days after the*
20 *date on which the Director receives information ob-*
21 *tained through a subpoena issued under this sub-*
22 *section, the Director shall notify any entity identified*
23 *by information obtained under the subpoena regard-*
24 *ing the subpoena and the identified vulnerability.*

25 “(6) *AUTHENTICATION.—*

1 “(A) *IN GENERAL.*—Any subpoena issued
2 by the Director under this subsection shall be au-
3 thenticated with a cryptographic digital signa-
4 ture of an authorized representative of the Agen-
5 cy, or other comparable successor technology,
6 that allows the recipient of the subpoena to deter-
7 mine that the subpoena was issued by the Agency
8 and has not been altered or modified since it was
9 issued by the Agency.

10 “(B) *INVALID IF NOT AUTHENTICATED.*—
11 Any subpoena issued by the Director under this
12 subsection that is not authenticated in accord-
13 ance with subparagraph (A) shall not be consid-
14 ered to be valid by the recipient of the subpoena.

15 “(7) *PROCEDURES.*—Not later than 90 days
16 after the date of enactment of this subsection, the Di-
17 rector shall establish internal procedures and associ-
18 ated training, applicable to employees and operations
19 of the Agency, regarding subpoenas issued under this
20 subsection, which shall address—

21 “(A) *the protection of and restriction on*
22 *dissemination of nonpublic information obtained*
23 *through a subpoena issued under this subsection,*
24 *including a requirement that the Agency shall*
25 *not disseminate nonpublic information obtained*

1 through a subpoena issued under this subsection
2 that identifies the party that is subject to the
3 subpoena or the entity at risk identified by in-
4 formation obtained, except that the Agency may
5 share the nonpublic information of the entity at
6 risk with another Federal agency if—

7 “(i) the Agency identifies or is notified
8 of a cybersecurity incident involving the en-
9 tity, which relates to the vulnerability
10 which led to the issuance of the subpoena;

11 “(ii) the Director determines that shar-
12 ing the nonpublic information with another
13 Federal agency is necessary to allow that
14 Federal agency to take a law enforcement or
15 national security action or actions related
16 to mitigating or otherwise resolving such in-
17 cident;

18 “(iii) the entity to which the informa-
19 tion pertains is notified of the Director’s de-
20 termination, to the extent practicable con-
21 sistent with national security or law en-
22 forcement interests; and

23 “(iv) the entity consents, except that
24 the entity’s consent shall not be required if
25 another Federal agency identifies the entity

1 to the Agency in connection with a sus-
2 pected cybersecurity incident;

3 “(B) the restriction on the use of informa-
4 tion obtained through the subpoena for a cyberse-
5 curity purpose, as defined in section 102 of the
6 Cybersecurity Information Sharing Act of 2015
7 (6 U.S.C. 1501);

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

11 “(i) destruction of information ob-
12 tained through the subpoena that the Direc-
13 tor determines is unrelated to critical infra-
14 structure immediately upon providing no-
15 tice to the entity pursuant to paragraph
16 (5); and

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

24 “(D) the processes for providing notice to
25 each party that is subject to the subpoena and

1 *each entity identified by information obtained*
2 *under a subpoena issued under this subsection;*

3 “(E) *the processes and criteria for con-*
4 *ducting critical infrastructure security risk as-*
5 *essments to determine whether a subpoena is*
6 *necessary prior to being issued under this sub-*
7 *section; and*

8 “(F) *the information to be provided to an*
9 *entity at risk at the time of the notice of the vul-*
10 *nerability, which shall include—*

11 “(i) *a discussion or statement that re-*
12 *sponding to, or subsequent engagement with,*
13 *the Agency, is voluntary; and*

14 “(ii) *to the extent practicable, informa-*
15 *tion regarding the process through which*
16 *the Director identifies security*
17 *vulnerabilities.*

18 “(8) *REVIEW OF PROCEDURES.—Not later than*
19 *1 year after the date of enactment of this subsection,*
20 *the Privacy Officer of the Agency shall—*

21 “(A) *review the procedures developed by the*
22 *Director under paragraph (7) to ensure that—*

23 “(i) *the procedures are consistent with*
24 *fair information practices; and*

1 “(ii) the operations of the Agency com-
2 ply with the procedures; and

3 “(B) notify the Committee on Homeland
4 Security and Governmental Affairs of the Senate
5 and the Committee on Homeland Security of the
6 House of Representatives of the results of the re-
7 view.

8 “(9) PUBLICATION OF INFORMATION.—Not later
9 than 120 days after establishing the internal proce-
10 dures under paragraph (7), the Director shall publish
11 information on the website of the Agency regarding
12 the subpoena process under this subsection, including
13 regarding—

14 “(A) the purpose for subpoenas issued under
15 this subsection;

16 “(B) the subpoena process;

17 “(C) the criteria for the critical infrastruc-
18 ture security risk assessment conducted prior to
19 issuing a subpoena;

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

22 “(E) guidelines on how entities contacted by
23 the Director may respond to notice of a sub-
24 poena; and

1 “(F) the procedures and policies of the
2 Agency developed under paragraph (7).

3 “(10) ANNUAL REPORTS.—The Director shall an-
4 nually submit to the Committee on Homeland Secu-
5 rity and Governmental Affairs of the Senate and the
6 Committee on Homeland Security of the House of
7 Representatives a report (which may include a classi-
8 fied annex but with the presumption of declassifica-
9 tion) on the use of subpoenas under this subsection by
10 the Director, which shall include—

11 “(A) a discussion of—

12 “(i) the effectiveness of the use of sub-
13 poenas to mitigate critical infrastructure se-
14 curity vulnerabilities;

15 “(ii) the critical infrastructure security
16 risk assessment process conducted for sub-
17 poenas issued under this subsection;

18 “(iii) the number of subpoenas issued
19 under this subsection by the Director during
20 the preceding year;

21 “(iv) to the extent practicable, the
22 number of vulnerable covered devices or sys-
23 tems mitigated under this subsection by the
24 Agency during the preceding year; and

1 “(v) the number of entities notified by
2 the Director under this subsection, and their
3 response, during the previous year; and

4 “(B) for each subpoena issued under this
5 subsection—

6 “(i) the source of the security vulner-
7 ability detected, identified, or received by
8 the Director;

9 “(ii) the steps taken to identify the en-
10 tity at risk prior to issuing the subpoena;
11 and

12 “(iii) a description of the outcome of
13 the subpoena, including discussion on the
14 resolution or mitigation of the critical in-
15 frastructure security vulnerability.

16 “(11) PUBLICATION OF THE ANNUAL REPORTS.—
17 The Director shall publish a version of the annual re-
18 port required by paragraph (10) on the website of the
19 Agency, which shall, at a minimum, include the find-
20 ings described in clauses (iii), (iv) and (v) of para-
21 graph (10)(A).

22 “(12) PROHIBITION ON USE OF INFORMATION
23 FOR UNAUTHORIZED PURPOSES.—Any information
24 obtained pursuant to a subpoena issued under this
25 subsection shall not be provided to any other Federal

1 *agency for any purpose other than a cybersecurity*
2 *purpose, as defined in section 102 of the Cybersecu-*
3 *rity Information Sharing Act of 2015 (6 U.S.C.*
4 *1501).”.*

5 *(b) RULES OF CONSTRUCTION.—*

6 *(1) PROHIBITION ON NEW REGULATORY AUTHOR-*
7 *ITY.—Nothing in this Act or the amendments made*
8 *by this Act shall be construed to grant the Secretary*
9 *of Homeland Security (in this subsection referred to*
10 *as the “Secretary”), or another Federal agency, any*
11 *authority to promulgate regulations or set standards*
12 *relating to the cybersecurity of private sector critical*
13 *infrastructure that was not in effect on the day before*
14 *the date of enactment of this Act.*

15 *(2) PRIVATE ENTITIES.—Nothing in this Act or*
16 *the amendments made by this Act shall be construed*
17 *to require any private entity—*

18 *(A) to request assistance from the Secretary;*

19 *or*

20 *(B) that requested such assistance from the*
21 *Secretary to implement any measure or rec-*
22 *ommendation suggested by the Secretary.*

Calendar No. 500

116TH CONGRESS
2^D SESSION

S. 3045

[Report No. 116-242]

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.

JULY 29, 2020

Reported with an amendment