

116TH CONGRESS  
1ST SESSION

**S.** \_\_\_\_\_

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

---

\_\_\_\_\_ introduced the following bill; which was read twice and 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 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 “\_\_\_\_\_ Act of  
5 \_\_\_\_\_”.

1 **SEC. 2. SUBPOENA AUTHORITY.**

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

4 (1) in subsection (c)—

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

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

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

10 “(12) detecting, identifying, and receiving infor-  
11 mation about security vulnerabilities relating to crit-  
12 ical infrastructure in the information systems and  
13 devices of Federal and non-Federal entities for a cy-  
14 bersecurity purpose, as defined in section 102 of the  
15 Cybersecurity Information Sharing Act of 2015 (6  
16 U.S.C. 1501).”; and

17 (2) by adding at the end the following:

18 “(n) SUBPOENA AUTHORITY.—

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

21 “(A) means a device or system commonly  
22 used to perform industrial, commercial, sci-  
23 entific, or governmental functions or processes  
24 that relate to critical infrastructure, including  
25 operational and industrial control systems, dis-

1           tributed control systems, and programmable  
2           logic controllers; and

3           “(B) does not include personal devices and  
4           systems.

5           “(2) AUTHORITY.—

6           “(A) IN GENERAL.—If the Director identi-  
7           fies a specific security vulnerability that relates  
8           to critical infrastructure and affects an enter-  
9           prise device or system used by a Federal or  
10          non-Federal entity, and the Director is unable  
11          to identify the entity at risk, the Director may  
12          issue a subpoena for the production of informa-  
13          tion necessary to identify and notify the entity  
14          at risk, in order to carry out a function author-  
15          ized under subsection (c)(12).

16          “(B) LIMIT ON INFORMATION.—A sub-  
17          poena issued under the authority under sub-  
18          paragraph (A) may only seek information in the  
19          categories set forth in subparagraphs (A), (B),  
20          (D), and (E) of section 2703(c)(2) of title 18,  
21          United States Code.

22          “(3) COORDINATION.—

23          “(A) IN GENERAL.—If the Director decides  
24          to exercise the subpoena authority under this  
25          subsection, and in the interest of avoiding inter-

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

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

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

17                   “(ii) subject to the limitations under  
18                   this subsection.

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

1       nership, corporation, association, or entity resides, is  
2       found, or transacts business.

3               “(5) NOTICE.—Not later than 7 days after the  
4       date on which the Director receives information ob-  
5       tained through a subpoena issued under this sub-  
6       section, the Director shall notify the subject of the  
7       subpoena regarding the subpoena.

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

14               “(A) the protection of and restriction on  
15       dissemination of nonpublic information obtained  
16       through a subpoena issued under this sub-  
17       section, including a requirement that nonpub-  
18       lically available information which is not related  
19       to the security vulnerability shall not be dis-  
20       seminated in a manner that identifies any  
21       United States person (as defined in section 101  
22       of the Foreign Intelligence Surveillance Act of  
23       1978 (50 U.S.C. 1801)), without the consent of  
24       the United States person;

1           “(B) the retention and destruction of non-  
2 public information obtained through a subpoena  
3 issued under this subsection, including—

4                   “(i) immediate destruction of informa-  
5 tion obtained through the subpoena that  
6 the Director determines is unrelated to  
7 critical infrastructure; and

8                   “(ii) destruction of any personally  
9 identifiable information not later than 6  
10 months after the date on which the Direc-  
11 tor receives information obtained through  
12 the subpoena, unless otherwise agreed to  
13 by the party identified by the subpoena re-  
14 spondent;

15           “(C) the processes for providing notice to  
16 the subjects of a subpoena issued under this  
17 subsection; and

18           “(D) the processes and criteria for con-  
19 ducting critical infrastructure security risk as-  
20 sessments to determine whether a subpoena is  
21 necessary prior to being issued under this sub-  
22 section.

23           “(7) REVIEW OF PROCEDURES.—Not later than  
24 1 year after the date of enactment of this sub-  
25 section, the Privacy Officer of the Agency shall—

1           “(A) review the procedures developed by  
2           the Director under paragraph (6) to ensure  
3           that—

4                   “(i) the procedures are consistent with  
5                   fair information practices; and

6                   “(ii) the operations of the Agency  
7                   comply with the procedures; and

8           “(B) notify the Committee on Homeland  
9           Security and Governmental Affairs of the Sen-  
10          ate and the Committee on Homeland Security  
11          of the House of Representatives of the results  
12          of the review.

13          “(8) PUBLICATION OF INFORMATION.—Not  
14          later than 120 days after establishing the internal  
15          procedures under paragraph (6), the Director shall  
16          make publicly available information regarding the  
17          subpoena process under this subsection, including  
18          regarding—

19                   “(A) the purpose for subpoenas issued  
20                   under this subsection;

21                   “(B) the subpoena process;

22                   “(C) the criteria for the critical infrastruc-  
23                   ture security risk assessment conducted prior to  
24                   issuing a subpoena;

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

3           “(E) guidelines on how entities contacted  
4           by the Director may respond to notice of a sub-  
5           poena; and

6           “(F) the procedures and policies of the  
7           Agency developed under paragraph (6).

8           “(9) ANNUAL REPORTS.—The Director shall  
9           annually submit to the Committee on Homeland Se-  
10          curity and Governmental Affairs of the Senate and  
11          the Committee on Homeland Security of the House  
12          of Representatives a report (which may include a  
13          classified annex but with the presumption of declas-  
14          sification) on the use of subpoenas under this sub-  
15          section by the Director, which shall include—

16               “(A) a discussion of—

17                   “(i) the effectiveness of the use of  
18                   subpoenas to mitigate critical infrastruc-  
19                   ture security vulnerabilities;

20                   “(ii) the critical infrastructure secu-  
21                   rity risk assessment process conducted for  
22                   subpoenas issued under this subsection;  
23                   and



1 “(iii) the number of subpoenas issued  
2 under this subsection by the Director dur-  
3 ing the preceding 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  
10 subject of the subpoena prior to issuing the  
11 subpoena; 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 (b) DEFINITION.—Section 2201 of the Homeland Se-  
17 curity Act of 2002 (6 U.S.C. 651) is amended—

18 (1) by redesignating paragraph (6) as para-  
19 graph (7); and

20 (2) by inserting after paragraph (5) the fol-  
21 lowing:

22 “(6) SECURITY VULNERABILITY.—The term  
23 ‘security vulnerability’ has the meaning given that  
24 term in section 102(17) of the Cybersecurity Infor-  
25 mation Sharing Act of 2015 (6 U.S.C. 1501(17)).”.