AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 500

116TH CONGRESS
2D 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.

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 2019''.

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

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

''(6) the term 'security vulnerability' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17));'';

(2) in subsection (c)—

(A) in paragraph (10), by striking ''and'' at the end;

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

(C) by adding at the end the following:

''(12) detecting, identifying, and receiving information about security vulnerabilities relating to crit-

ical infrastructure in the information systems and devices of Federal and non-Federal entities for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).''; and

(3) by adding at the end the following:

''(n) SUBPOENA AUTHORITY.—

''(1) DEFINITION.—In this subsection, the term 'enterprise device or system'—

''(A) means a device or 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.

''(2) AUTHORITY.—

''(A) IN GENERAL.—If the Director identifies a 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 owned or operated by a Federal or non-Federal entity, and the Director is unable to identify the entity at risk, 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 function authorized under subsection (c)(12).

''(B) LIMIT ON INFORMATION.—A subpoena issued under the authority under subparagraph (A) 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.

''(C) LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.—The provisions of section 2703(c) of title 18, United States Code, shall apply to any subpoena issued under the authority under subparagraph (A).

''(3) COORDINATION.—

''(A) IN GENERAL.—If the Director decides to exercise the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall coordinate the issuance

of any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to inter-agency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after the date of enactment of this subsection.

"(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 in order to carry out a function described in subsection (c)(12); and

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

"(4) 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.

"(5) NOTICE.—Not later than 7 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 vulnerability.

"(6) 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.

"(7) PROCEDURES.—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—

"(A) the protection of and restriction on dissemination of nonpublic information obtained through a subpoena issued under this subsection, including a requirement that the Agency shall not disseminate nonpublic information obtained through a subpoena issued under this

subsection that identifies the party that is subject to the subpoena or the entity at risk identified by information obtained, 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 vulnerability which led to the issuance of the subpoena;

"(B) the restriction on the use of information obtained through the subpoena for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);

"(C) the retention and destruction of nonpublic information obtained through a subpoena issued under this subsection, including—

"(i) immediate destruction of information obtained through the subpoena that the Director determines is unrelated to critical infrastructure; and

"(ii) destruction of any personally identifiable information not later than 6 months after the date on which the Director receives information obtained through

the subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent;

"(D) the processes for providing notice to each party that is subject to the subpoena and each entity at risk identified by information obtained pursuant to a subpoena issued under this subsection; and

"(E) the processes and criteria for conducting critical infrastructure security risk assessments to determine whether a subpoena is necessary prior to being issued under this subsection.

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

"(A) review the procedures developed by the Director under paragraph (7) to ensure that—

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

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

"(B) notify the Committee on Homeland Security and Governmental Affairs of the Sen-

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

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

"(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) guidelines on how entities contacted by the Director may respond to notice of a subpoena; and

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

"(10) ANNUAL REPORTS.—The Director shall annually submit 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—

''(A) a discussion of—

''(i) the effectiveness of the use of subpoenas to mitigate critical infrastructure 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; and

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

''(B) for each subpoena issued under this subsection—

~~"(i) the source of the security vulnerability detected, identified, or received by the Director;~~

~~"(ii) the steps taken to identify the entity at risk prior to issuing the subpoena; and~~

~~"(iii) a description of the outcome of the subpoena, including discussion on the resolution or mitigation of the critical infrastructure security vulnerability.~~

~~"(11) PUBLICATION OF THE ANNUAL REPORTS.—The Director shall make a version of the annual report required by paragraph (10) publicly available, which shall, at a minimum, include the findings described in clause (iii), (iv) and (v) of subparagraph (A).".~~

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 paragraph (5), by striking "and" at the end;

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

(C) by inserting after paragraph (5) the following:

"(6) the term 'security vulnerability' has the meaning given that term in section 102(17) of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(17)); and";

(2) in subsection (c)—

(A) in paragraph (10), by striking "and" at the end;

(B) in paragraph (11), by striking the period at the end and inserting "; and"; and

(C) by adding at the end the following:

"(12) detecting, identifying, and receiving information about security vulnerabilities relating to critical infrastructure in the information systems and devices of Federal and non-Federal entities for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501)."; and

(3) by adding at the end the following:

"(o) SUBPOENA AUTHORITY.—

"(1) DEFINITION.—In this subsection, the term 'covered device or system'—

"(A) means a device or 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.

"(2) AUTHORITY.—

"(A) IN GENERAL.—If the Director identifies a 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 a covered device or system owned or operated by a Federal or non-Federal entity, and the Director is unable to identify the entity at risk, 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 function authorized under subsection (c)(12).

"(B) LIMIT ON INFORMATION.—A subpoena issued under the authority under subparagraph (A) may seek information—

"(i) only in the categories set forth in subparagraphs (A), (B), (D), and (E) of section 2703(c)(2) of title 18, United States Code; and

"(ii) for not more than 20 covered devices or systems.

"(C) LIABILITY PROTECTIONS FOR DISCLOSING PROVIDERS.—The provisions of section 2703(e) of title 18, United States Code, shall apply to any subpoena issued under the authority under subparagraph (A).

"(3) COORDINATION.—

"(A) IN GENERAL.—If the Director decides to exercise the subpoena authority under this subsection, and in the interest of avoiding interference with ongoing law enforcement investigations, the Director shall coordinate the issuance of any such subpoena with the Department of Justice, including the Federal Bureau of Investigation, pursuant to inter-agency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60

days after the date of enactment of this subsection.

"(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 in order to carry out a function described in subsection (c)(12); and

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

"(4) 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.

"(5) NOTICE.—Not later than 7 days after the date on which the Director receives information obtained through a subpoena issued under this subsection, the Director shall notify any entity identified by information obtained under the subpoena regarding the subpoena and the identified vulnerability.

"(6) AUTHENTICATION.—

"(A) IN GENERAL.—Any subpoena issued by the Director under this subsection shall be authenticated with a cryptographic digital signature of an authorized representative of the Agency, or other comparable successor technology, that allows the recipient of the subpoena to determine that the subpoena was issued by the Agency and has not been altered or modified since it was issued by the Agency.

"(B) INVALID IF NOT AUTHENTICATED.—Any subpoena issued by the Director under this subsection that is not authenticated in accordance with subparagraph (A) shall not be considered to be valid by the recipient of the subpoena.

"(7) PROCEDURES.—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—

"(A) the protection of and restriction on dissemination of nonpublic information obtained through a subpoena issued under this subsection, including a requirement that the Agency shall not disseminate nonpublic information obtained

through a subpoena issued under this subsection that identifies the party that is subject to the subpoena or the entity at risk identified by information obtained, except that the Agency may share the nonpublic information of the entity at risk with another Federal agency if—

"(i) the Agency identifies or is notified of a cybersecurity incident involving the entity, which relates to the vulnerability which led to the issuance of the subpoena;

"(ii) the Director determines that sharing the nonpublic information with another Federal agency is necessary to allow that Federal agency to take a law enforcement or national security action or actions related to mitigating or otherwise resolving such incident;

"(iii) the entity to which the information pertains is notified of the Director's determination, to the extent practicable consistent with national security or law enforcement interests; and

"(iv) the entity consents, except that the entity's consent shall not be required if another Federal agency identifies the entity

to the Agency in connection with a suspected cybersecurity incident;

"(B) the restriction on the use of information obtained through the subpoena for a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501);

"(C) the retention and destruction of nonpublic information obtained through a subpoena issued under this subsection, including—

"(i) destruction of information obtained through the subpoena that the Director determines is unrelated to critical infrastructure immediately upon providing notice to the entity pursuant to paragraph (5); and

"(ii) destruction of any personally identifiable information not later than 6 months after the date on which the Director receives information obtained through the subpoena, unless otherwise agreed to by the individual identified by the subpoena respondent;

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

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

"(E) the processes and criteria for conducting critical infrastructure security risk assessments to determine whether a subpoena is necessary prior to being issued under this subsection; and

"(F) the information to be provided to an entity at risk at the time of the notice of the vulnerability, which shall include—

"(i) a discussion or statement that responding to, or subsequent engagement with, the Agency, is voluntary; and

"(ii) to the extent practicable, information regarding the process through which the Director identifies security vulnerabilities.

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

"(A) review the procedures developed by the Director under paragraph (7) to ensure that—

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

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

"(B) notify the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives of the results of the review.

"(9) PUBLICATION OF INFORMATION.—Not later than 120 days after establishing the internal procedures under paragraph (7), the Director shall publish information on the website of the Agency regarding the subpoena process under this subsection, including regarding—

"(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) guidelines on how entities contacted by the Director may respond to notice of a subpoena; and

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

"(10) ANNUAL REPORTS.—The Director shall annually submit 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—

"(A) a discussion of—

"(i) the effectiveness of the use of subpoenas to mitigate critical infrastructure 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 covered devices or systems mitigated under this subsection by the Agency during the preceding year; and

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

"(B) for each subpoena issued under this subsection—

"(i) the source of the security vulnerability detected, identified, or received by the Director;

"(ii) the steps taken to identify the entity at risk prior to issuing the subpoena; and

"(iii) a description of the outcome of the subpoena, including discussion on the resolution or mitigation of the critical infrastructure security vulnerability.

"(11) PUBLICATION OF THE ANNUAL REPORTS.—The Director shall publish a version of the annual report required by paragraph (10) on the website of the Agency, which shall, at a minimum, include the findings described in clauses (iii), (iv) and (v) of paragraph (10)(A).

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

agency for any purpose other than a cybersecurity purpose, as defined in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).".

(b) RULES OF CONSTRUCTION.—

(1) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this Act or the amendments made by this Act shall be construed to grant the Secretary of Homeland Security (in this subsection referred to as the "Secretary"), or another Federal agency, any authority to promulgate regulations or set standards relating to the cybersecurity of private sector critical infrastructure that was not in effect on the day before the date of enactment of this Act.

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

(A) to request assistance from the Secretary; or

(B) that requested such assistance from the Secretary to implement any measure or recommendation suggested by the Secretary.

Calendar No. 500

116TH CONGRESS
2D 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