AMENDMENT TO RULES COMM. PRINT 116–57
OFFERED BY MR. LANGEVIN OF RHODE ISLAND

Add at the end of subtitle C of title XVI the following:

SEC. 16___. 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 paragraphs (1) through (6) as paragraphs (2) through (7), respectively;

(B) by inserting before paragraph (2), as so redesignated, the following new paragraph:

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

(C) in paragraph (6), as so redesignated, by striking ''and'' at the end;

(D) by redesignating paragraph (7), as so redesignated, as paragraph (8); and

(E) by inserting after paragraph (6), as so redesignated, the following new paragraph:

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

''(12) detecting, identifying, and receiving information for a cybersecurity purpose about security vulnerabilities relating to critical infrastructure in information systems and devices.''; and

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

''(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, dis-

tributed 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 such security vulnerability relates to critical infrastructure and affects a covered device or system, and the Director is unable to identify the entity at risk that owns or operates such covered device or system, the Director may issue a subpoena for the production of information necessary to identify and notify such entity at risk, in order to carry out a function authorized under subsection (c)(12).

''(B) LIMIT ON INFORMATION.—A subpoena issued pursuant to 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 pursuant to subparagraph (A).

''(3) COORDINATION.—

''(A) IN GENERAL.—If the Director exercises 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 interagency procedures which the Director, in coordination with the Attorney General, shall develop not later than 60 days after the date of the enactment of this subsection.

''(B) CONTENTS.—The inter-agency procedures developed under this paragraph shall pro-

vide that a subpoena issued by the Director under this subsection shall be—

''(i) issued to carry out a function described in subsection (c)(12); and

''(ii) subject to the limitations specified in this subsection.

''(4) NONCOMPLIANCE.—If any person, partnership, corporation, association, or entity fails to comply with any duly served subpoena issued pursuant to this subsection, the Director may request that the Attorney General seek enforcement of such 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 seven days after the date on which the Director receives information obtained through a subpoena issued pursuant to this subsection, the Director shall notify any entity identified by information obtained pursuant to such subpoena regarding such subpoena and the identified vulnerability.

''(6) AUTHENTICATION.—

''(A) IN GENERAL.—Any subpoena issued pursuant to 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 Agency to demonstrate that such subpoena was issued by the Agency and has not been altered or modified since such issuance.

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

''(7) PROCEDURES.—Not later than 90 days after the date of the enactment of this subsection, the Director shall establish internal procedures and associated training, applicable to employees and operations of the Agency, regarding subpoenas issued pursuant to this subsection, which shall address the following:

''(A) The protection of and restriction on dissemination of nonpublic information obtained through such a subpoena, including a requirement that the Agency not disseminate nonpublic information obtained through such a subpoena that identifies the party that is subject to such subpoena or the entity at risk identified by information obtained, except that the Agency

may share the nonpublic information with the Department of Justice for the purpose of enforcing such subpoena in accordance with paragraph (4), and may share with a Federal agency the nonpublic information of the entity at risk if—

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

''(ii) the Director determines that sharing the nonpublic information with another Federal department or agency is necessary to allow such department or agency to take a law enforcement or national security action, consistent with the interagency procedures under paragraph (3)(A), 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 en-

forcement interests, consistent with such interagency procedures; and

''(iv) the entity consents, except that the entity's consent shall not be required if another Federal department or agency identifies the entity to the Agency in connection with a suspected cybersecurity incident.

''(B) The restriction on the use of information obtained through such a subpoena for a cybersecurity purpose.

''(C) The retention and destruction of nonpublic information obtained through such a subpoena, including—

''(i) destruction of such information 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 six months after the date on which the Director receives information obtained through such a 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 such a subpoena and each entity identified by information obtained under such a subpoena.

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

''(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) LIMITATION ON PROCEDURES.—The internal procedures established pursuant to paragraph (7) may not require an owner or operator of critical

infrastructure to take any action as a result of a notice of vulnerability made pursuant to this Act.

''(9) REVIEW OF PROCEDURES.—Not later than one year after the date of the enactment of this subsection, the Privacy Officer of the Agency shall—

''(A) review the internal procedures established pursuant to paragraph (7) to ensure that—

''(i) such procedures are consistent with fair information practices; and

''(ii) the operations of the Agency comply with such 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 under subparagraph (A).

''(10) 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 information regarding the following:

''(A) Such internal procedures.

''(B) The purpose for subpoenas issued pursuant to this subsection.

''(C) The subpoena process.

''(D) The criteria for the critical infrastructure security risk assessment conducted prior to issuing a subpoena.

''(E) Policies and procedures on retention and sharing of data obtained by subpoenas.

''(F) Guidelines on how entities contacted by the Director may respond to notice of a subpoena.

''(11) 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 issued pursuant to this subsection, which shall include the following:

''(A) A discussion of the following:

''(i) The effectiveness of the use of such 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 so issued 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.

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

''(B) For each subpoena issued pursuant to this subsection, the following:

''(i) Information relating to the source of the security vulnerability detected, identified, or received by the Director.

''(ii) Information relating to the steps taken to identify the entity at risk prior to issuing the subpoena.

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

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

"(13) PROHIBITION ON USE OF INFORMATION FOR UNAUTHORIZED PURPOSES.—Any information obtained pursuant to a subpoena issued under this subsection may not be provided to any other Federal department or agency for any purpose other than a cybersecurity purpose or for the purpose of enforcing a subpoena issued pursuant to this subsection.".

(b) RULES OF CONSTRUCTION.—

(1) PROHIBITION ON NEW REGULATORY AUTHORITY.—Nothing in this section or the amendments made by this section may be construed to grant the Secretary of Homeland Security, or the head of any another Federal agency or department, 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 the enactment of this Act.

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

(A) to request assistance from the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security; or

(B) implement any measure or recommendation suggested by the Director.