AMENDMENT TO RULES COMM. PRINT 119–33

OFFERED BY M__. _____

Add at the end of subtitle A of title XVII the following:

SEC. 17___. DHS RESPONSIBILITIES RELATING TO VULNERABILITY DATA.

(a) RESPONSIBILITIES OF THE DIRECTOR OF CISA.—Subsection (c) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended—

(1) in paragraph (13), by striking ''and'' after the semicolon;

(2) by redesignating paragraph (14) as paragraph (16); and

(3) by inserting after paragraph (13) the following new paragraphs:

''(14) facilitate the development, management, enrichment, publication, and cataloguing of data relating to vulnerabilities, and make such data available to the public at no cost to identify systemic risks to software operators, recurring classifications of vulnerabilities, and opportunities to improve software safety;

''(15) conduct analyses of vulnerabilities to identify systemic risks to software operators, recurring classifications of vulnerabilities, opportunities to improve software safety, and support vulnerability enrichment, and make such analyses available to the public at no cost; and''.

(b) CISA SUPPORT FOR COMMON VULNERABILITY DATA.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended by adding at the end the following new subsection:

''(t) COMMON VULNERABILITIES AND EXPOSURE PROGRAM.—

''(1) IN GENERAL.—There is in the Center the Common Vulnerabilities and Exposures (CVE) Program (in this subsection referred to as the 'CVE Program'), which shall support the development, management, enrichment, publication, and cataloguing of vulnerability data to carry out the following:

''(A) Enable mitigation of, prioritization of, and communication regarding vulnerabilities.

''(B) Support analyses to identify systemic risks to software operators, recurring vulnerability classes, and opportunities to improve software safety.

''(2) AGENCY RESPONSIBILITIES.—

''(A) IN GENERAL.—The Director shall carry out the Program, including by—

''(i) supporting the duties of the CVE Board pursuant to paragraph (5)(B); and

''(ii) maintaining the infrastructure of the Program.

''(B) SUPPORT.—The Director of the National Institute of Standards and Technology shall support the Program through technical assistance, standards development activities, and tool development.

''(3) OPERATING ENTITY.—The Center shall designate one or more 'Operating Entities', which may include the Center or nongovernmental organizations, including federally funded research and development centers, with which the Center enters into cooperative agreements to be responsible for day-to-day operations of the CVE Program.

''(4) REQUIREMENTS.—An Operating Entity shall, pursuant to a cooperative agreement under paragraph (2), carry out the following:

''(A) Manage a CVE catalogue of standardized vulnerability data submitted by certified CVE Numbering Authorities and other entities

to satisfy the vulnerability identification needs of the global cybersecurity community.

''(B) Certify and decertify CVE Numbering Authorities.

''(C) Maintain and periodically update the technical infrastructure of the CVE Program, including relating to the automation of data transfers, machine readable formats, and usage of application program interfaces, and other technologies to facilitate catalogue usage by industry.

''(D) Administer training for CVE Numbering Authorities required to maintain certification.

''(E) Hire and manage staff as required to carry out the requirements of this paragraph.

''(F) Carry out such other activities as necessary for the administration of the CVE Program, as directed by the CVE Board under paragraph (5).

''(5) COMMON VULNERABILITIES AND EXPOSURES BOARD.—

''(A) IN GENERAL.—There is in the CVE Program the Common Vulnerabilities and Exposures Board (in this subsection referred to as

the 'CVE Board'). The CVE Board shall develop, evaluate, oversee, and update, as appropriate, the policies and procedures of the CVE Program.

''(B) DUTIES.—The CVE Board shall be responsible for the following:

''(i) Establishing bylaws for the CVE Board and the CVE Program in accordance with subparagraph (C).

''(ii) Providing overall strategic direction for the activities of the CVE Program, including any Operating Entities designated pursuant to paragraph (3), and establishing priority activities.

''(iii) Establishing policies, guidance, and criteria related to all aspects of the CVE Program, including for the following:

''(I) Top-Level Root CVE Numbering Authorities, including procedures to certify and decertify Top-Level Root CVE Numbering Authorities.

''(II) CVE Numbering Authorities, including procedures to certify

and decertify CVE Numbering Authorities.

''(III) CVE Records, including specifying minimum requirements for such records.

''(IV) Written standards to govern the ownership and licensing of any intellectual property rights developed by the CVE Program or derived from collaborative efforts of the CVE Program that protect the continuity of the CVE Program.

''(V) Written guidelines relating to privacy and civil liberties that govern the development, management, enrichment, publication, and cataloguing of vulnerability data obtained in connection with the CVE Program.

''(VI) The establishment of expert working groups to issue updates to the CVE Program, including expanding or contracting the scope of vulnerabilities collected (such as relating to misconfigurations or weaknesses) and any related required data.

''(VII) Providing appropriate representation on and engagement with international boards to ensure interoperability and preeminence of the CVE Program.

''(iv) Training for CVE Numbering Authorities.

''(v) Evaluating the performance of the CVE Program, including by establishing a process to measure the use and quality of CVE Records.

''(C) BYLAWS.—The CVE Board shall establish bylaws and ensure the following:

''(i) Such bylaws include policies relating to the following:

''(I) Ethical and disclosure standards.

''(II) Standards of conduct.

''(III) Financial disclosure statements.

''(IV) Conflicts of interest, including recusal and waiver rules.

''(V) Audits.

''(VI) Attendance requirements.

''(VII) Any other matters determined appropriate by the CVE Board.

''(ii) Such bylaws, and activities carried out pursuant to such bylaws, do not compromise, or appear to compromise, the integrity of any government agency or program, or any officer or employee employed by such an agency, or involved in such a program.

''(D) COMPOSITION.—The CVE Board shall be composed of 15 members, of whom not more than seven such members shall be permanent members and the remainder of such members shall be rotating members, as follows:

''(i) PERMANENT MEMBERS.—Permanent members of the CVE Board shall include the following:

''(I) The Director.

''(II) The Director of the National Institute of Standards and Technology.

''(III) Top-Level Root CVE Numbering Authorities, or successor designation, as determined by the Director.

''(ii) ROTATING MEMBERS.—Rotating members of the CVE Board shall have relevant expertise in the CVE Program or related issues, and shall include the following:

''(I) Officials of foreign governments determined appropriate by the Director.

''(II) Representatives of CVE Numbering Authorities.

''(III) Representatives of academia and security researchers community.

''(IV) Representatives of the private sector, including private sector entities that rely on CVE records.

''(V) Representatives of international standards and governance organizations determined appropriate by the Director.

''(VI) Individuals with expertise in open-source software.

''(VII) Individuals with expertise in operational technology.

''(VIII) Other individuals with relevant expertise, as determined appropriate by the Director.

''(E) CO-CHAIRS.—Members of the CVE Board shall elect one government official and one nongovernment official to serve as co-chairs of the CVE Board. The co-chairs shall serve for a term of two years, and may be re-elected to a second two-year term. The co-chairs shall be responsible for the following:

''(i) Scheduling meetings of the CVE Board.

''(ii) Setting the agenda for CVE Board meetings.

''(iii) Facilitating CVE Board consideration of recommendations related to improving the CVE Program.

''(iv) Making publicly available written summaries of CVE Board meetings.

''(F) MEMBER SELECTION.—

''(i) IN GENERAL.—The Director shall appoint members of the CVE Board in accordance with subparagraph (G).

''(ii) EXPERIENCE.—The Director shall ensure the appointed members of the

CVE Board have appropriate experience and are qualified to provide advice and information relating to the field of vulnerability management and reporting.

''(iii) CONSIDERATION.—In appointing members of the CVE Board, the Director shall seek and give consideration to recommendations from the Secretary of Commerce, Congress, industry, academia, nonprofit organizations, the defense community, other appropriate organizations, and sitting members of the CVE Board.

''(G) TERMS AND VACANCIES.—

''(i) TERM LENGTH.—Except as provided in clause (ii), the term of office of each rotating member of the CVE Board shall be for five years, except that such a member may continue to serve after the expiration of the term of such member until the expiration of the 180-day period beginning on the date on which such term of such member would otherwise expire, if no new member is appointed to replace such departing member.

"(ii) INITIAL APPOINTED MEMBERS.—Of the initial rotating members of the CVE Board appointed under subparagraph (F)—

"(I) half, or in the case of an odd number of such members, one fewer than half of such members, shall—

"(aa) be appointed by not later than 60 days after the date of the enactment of this subsection; and

"(bb) serve for three years, as determined by the co-chairs;

"(II) half, or in the case of an odd number of such members, one more than half of such members, shall—

"(aa) be appointed by not later than 60 days after the date of the enactment of this subsection; and

"(bb) serve for five years, as determined by the co-chairs; and

"(III) at least five of such members shall be appointed from the CVE

Board as in existence as of the date of the enactment of this subsection.

''(iii) TERM LIMITS.—Rotating members of the CVE Board may serve not more than two consecutive terms.

''(iv) VACANCIES.—A vacancy on the CVE Board shall be filled in the same manner in which the original appointment was made.

''(v) REMOVAL.—The Director may not remove any member except for inefficiency, neglect of duty, malfeasance, or other violation of policies specified in subparagraph (C)(i).

''(vi) QUORUM.—

''(I) IN GENERAL.—A majority of the members of the CVE Board shall constitute a quorum for the purposes of conducting the business of the CVE Board.

''(II) RECUSAL.—A member of the CVE Board who seeks recusal due to a conflict of interest referred to in subparagraph (C)(i)(IV) shall be con-

sidered present for purposes of establishing a quorum.

''(H) COMPENSATION.—

''(i) IN GENERAL.—Non-Federal members of the CVE Board may not receive compensation for serving on the CVE Board.

''(ii) CERTAIN EXPENSES.—Non-Federal members of the CVE Board may be reimbursed for travel expenses, including per diem in lieu of subsistence, and other necessary expenses incurred in carrying out the duties of the CVE Board.

''(I) PUBLIC MEETING.—The CVE Board shall hold a public meeting not less frequently than once every four months. Each such meeting shall be made available to the public on a website of the Agency.

''(6) ASSESSMENT.—

''(A) IN GENERAL.—Not later than nine months after the date of the enactment of this subsection, the CVE Board shall submit to the appropriate congressional committees an assessment of the CVE Program. The Assessment shall include information on the following:

''(i) The ability of existing funds appropriated or otherwise made available to ensure the long-term stability of the CVE Program.

''(ii) The quality and scope of existing CVE Record requirements, and whether such requirements generate sufficient information to aid the global cybersecurity community in the mitigation of vulnerabilities, cybersecurity threats, and cybersecurity risks.

''(iii) Existing CVE Record enrichment practices.

''(iv) Existing criteria to certify or decertify a CVE Numbering Authority.

''(v) The quality of existing guidance and training resources for CVE Numbering Authorities.

''(vi) Existing mechanisms to ensure CVE Program transparency.

''(vii) Existing guidelines relating to privacy and civil liberties governing the CVE Program.

''(viii) Existing mechanisms to gather feedback and recommendations to improve the CVE Program.

''(B) PUBLICATION.—The CVE Board shall make copies of the assessment submitted under subparagraph (A) available—

''(i) for public inspection, and shall upon request provide a copy of such assessment to any individual for a charge not to exceed the cost of providing such copy; and

''(ii) to the appropriate congressional committees.

''(7) NONAPPLICABILITY.—Chapter 10 of title 5, United States Code, and section 3507 of title 44, United States Code, shall not apply to the CVE Program, CVE Board, or any components thereof.

''(8) ADMINISTRATIVE CONTROL.—No appointed member of the CVE Board, officer or employee of a designated Operating Entity that is a nongovernmental entity, or participant in the CVE Program may exercise administrative control over any Federal employee.

''(9) DETERMINATION.—If the Director determines such is appropriate, the Director may carry

out this subsection, or any provision of this subsection, as part of any existing contract, structure, activity, or partnership of the Center.

''(10) APPROPRIATIONS.—

''(A) AVAILABILITY.—Amounts authorized to be appropriated to carry out this subsection are authorized to be made available until expended.

''(B) CONTRIBUTION OF FUNDS AND SERVICES BY FOREIGN GOVERNMENTS, INTERNATIONALS ORGANIZATIONS, AND NONGOVERNMENTAL ORGANIZATIONS.—The Director shall encourage foreign governments, international organizations, and nongovernmental organizations to participate to the maximum extent feasible in carrying out this subsection, and to make contributions of funds and services which the Director is authorized to accept, to be utilized to so carry out this subsection.

''(11) DEFINITIONS.—In this subsection:

''(A) CVE CATALOGUE.—The term 'CVE catalogue' means a list of entries, each of which contains an identification number, a description, and at least one public reference for publicly known cybersecurity vulnerabilities.

''(B) CVE ID.—The term 'CVE ID' means a unique, standardized alphanumeric string that identifies a specific publicly disclosed cybersecurity vulnerability.

''(C) CVE NUMBERING AUTHORITY.—The term 'CVE Numbering Authority' means a vendor, researcher, open source project, Computer Emergency Response Team (CERT), hosted service, bug bounty provider, or consortium organization authorized by the CVE Program to assign CVE IDs to vulnerabilities and publish CVE Records.

''(D) CVE RECORD.—The term 'CVE Numbering Record' means structured vulnerability data regarding a vulnerability associated with a CVE ID assigned by a CVE Numbering Authority.

''(E) ENRICHMENT.—The term 'enrichment' means adding information beyond the minimum requirements under paragraph (5)(B)(iii)(III) for a CVE Record established by the CVE Board, including intelligence or information regarding contextual risk severity and active exploitation of a vulnerability described in a CVE Record, and tactics, techniques, or

procedures involved in such exploits, or public reporting of such.

''(F) SECURITY RESEARCHER.—The term 'security researcher' means an individual who investigates, studies, and analyzes vulnerabilities, cybersecurity threats, and cybersecurity risks, and shares that information learned as a result of such investigation, study, and analysis to mitigate vulnerabilities, cybersecurity threats, and cybersecurity risks.

''(G) TOP-LEVEL ROOT CVE NUMBERING AUTHORITY.—The term 'Top-Level Root CVE Numbering Authority' means an entity responsible for governing CVE Numbering Authorities within designated domains that meet the requirements established by the Board or that was designated as a Top-Level Root CVE Numbering Authority before the date of the enactment of this subsection.

''(H) VULNERABILITY.—The term 'vulnerability' means a weakness in the computational logic, misconfiguration, or other attribute found in software, shared cloud services, firmware, or hardware components that, when exploited, results in a negative impact to confidentiality, in-

tegrity, or availability of an information system product or service.''.

(c) JOINT STRATEGIC PLAN.—

(1) DEVELOPMENT.—

(A) IN GENERAL.—Not later than 18 months after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security and the Director of the National Institute of Standards and Technology shall jointly develop a strategic plan (in this subsection referred to as the ''strategic plan'') for the modernization and long-term sustainability of the CVE Program under subsection (t) of section 2209 of the Homeland Security Act of 2002, as added by subsection (b).

(B) PURPOSES.—The purposes of the strategic plan are the following:

(i) To modernize the CVE Program referred to in subparagraph (A) to streamline—

(I) Federal efforts that support the development, management, enrichment, publication, and cataloguing of vulnerability data; and

(II) the National Vulnerability Database maintained by the National Institute of Standards and Technology.

(ii) To improve service delivery and vulnerability data quality, including completeness, accuracy, and timeliness of records.

(iii) To ensure transparent, neutral, effective, and multistakeholder governance of the CVE Program, including by increasing international participation in governance structures.

(iv) To promote long-term sustainability of the CVE Program, including through potential contributions from other funding sources.

(C) ELEMENTS.—Taking into consideration the findings of the assessment under section 2209(t)(6) of the Homeland Security Act of 2002, as added by subsection (b), the strategic plan shall include the following:

(i) A cost assessment for implementing the strategic plan and sustaining the CVE Program referred to in subpara-

graph (A) and he National Vulnerability Database over ten years, including mechanisms to leverage resources provided by CVE Program stakeholders and partners.

(ii) A description detailing the roles and responsibilities of the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Institute of Standards and Technology, that align with the distinct missions of each such Director, to implement a plan to transition to the CVE Program or otherwise streamline the National Vulnerability Database maintained by the National Institute of Standards and Technology, as appropriate, in accordance with subparagraph (B)(i)(II).

(iii) A description of activities to improve, scale, and streamline the development, management, enrichment, publication, and cataloguing of vulnerability data.

(iv) A plan for enhancing the governance of the CVE Program to improve data quality, multistakeholder participation, and service delivery.

(v) A strategy for engagement with international allies and partners on activities that support the development, management, enrichment, publication, and cataloguing of vulnerability data.

(vi) Recommendations for administrative and legislative action that could optimize the effectiveness of the CVE Program and the National Vulnerability Database.

(D) STAKEHOLDER COLLABORATION.—In developing the strategic plan, the Director of the Cybersecurity and Infrastructure Security Agency and the Director of the National Institute of Standards and Technology shall seek input from other Federal departments and agencies, academia, civil society organizations, private sector stakeholders, nonprofit organizations, and other organizations, as appropriate.

(2) SUBMISSION TO CONGRESS.—Not later than 18 months after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the appropriate congressional committees—

(A) the strategic plan; and

(B) an implementation plan for the strategic plan.

(3) DEFINITIONS.—In this subsection:

(A) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term ''appropriate congressional committees'' means—

(i) the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives; and

(ii) the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate.

(B) ENRICHMENT.—The term ''enrichment'' has the meaning given such term in subsection (t) of section 2209 of the Homeland Security Act of 2002, as added by subsection (b).

(C) NATIONAL VULNERABILITY DATABASE.—The term ''National Vulnerability Database'' means the publicly available database of vulnerability management data comprising known vulnerabilities and related data supported by the National Institute of Standards and Technology.

(D) VULNERABILITY.—The term ''vulnerability'' has the meaning given such term in subsection (t) of section 2209 of the Homeland Security Act of 2002, as added by subsection (b).

☒