AMENDMENT TO RULES COMM. PRINT 117–54
OFFERED BY MR. LANGEVIN OF RHODE ISLAND

Add at the end of title LII of division E the following:

SEC. 52___. OFFICE OF CYBERSECURITY STATISTICS.

(a) IN GENERAL.—Subtitle A of title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended by adding at the end the following:

"SEC. 2220E. OFFICE OF CYBERSECURITY STATISTICS.

''(a) DEFINITIONS.—In this section:

''(1) AGENCY.—The term 'Agency' means the Cybersecurity and Infrastructure Security Agency.

''(2) CENTER.—The term 'Center' means the Federal information security incident center described in section 3556 of title 44, United States Code.

''(3) COVERED CLAIM.—The term 'covered claim' means an insurance claim paid by an insurance provider as a result of an insured cyber incident loss.

''(4) CYBER INCIDENT.—The term 'cyber incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the in-

tegrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system, including relating to the following:

''(A) Unauthorized access to an information system or network that leads to loss of confidentiality, integrity, or availability of such information system or network.

''(B) Disruption of business operations due to a distributed denial of service attack against an information system or network.

''(C) Unauthorized access or disruption of business operations due to loss of service facilitated through, or caused by a cloud service provider, managed service provider, or other data hosting provider.

''(D) Fraudulent or malicious use of a cloud service account, data hosting account, internet service account, or any other digital service.

''(5) CYBER THREAT INDICATOR.—The term 'cyber threat indicator' has the meaning given such term in section 102 of the Cybersecurity Act of 2015 (6 U.S.C. 1501; enacted as division N of the Con-

solidated Appropriations Act, 2016 (Public Law 114–113).

''(6) DIRECTOR.—The term Director means the Director of the Office.

''(7) INFORMATION SYSTEM.—The term 'information system'—

''(A) has the meaning given the term in section 3502 of title 44, United States Code; and

''(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers.

''(8) INSURANCE PROVIDER.—The term 'insurance provider' means any nongovernmental organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture (without regard to whether it is established for profit) that is engaged in or affecting interstate commerce and that provides insurance products to cover losses associated with a cyber incident.

''(9) OFFICE.—The term 'Office' means the Office of Cybersecurity Statistics established under subsection (b).

''(10) STATISTICAL PURPOSE.—The term 'statistical purpose'—

''(A) means the description, estimation, or analysis of the characteristics of groups, without identifying the individuals or organizations that comprise such groups; and

''(B) includes the development, implementation, or maintenance of methods, technical or administrative procedures, or information resources that support the purposes described in subsection (c).

''(b) ESTABLISHMENT.—There is established within the Agency an Office of Cybersecurity Statistics.

''(c) DIRECTOR.—

''(1) IN GENERAL.—The Office shall be headed by a Director, who shall report to the Director of the Agency.

''(2) AUTHORITY.—The Director shall—

''(A) have final authority for all cooperative agreements and contracts awarded by the Office;

''(B) be responsible for the integrity of data and statistics collected or issued by the Office; and

''(C) protect against improper or unlawful use or disclosure of information furnished for exclusively statistical purposes under this section, consistent with the requirements of subsection (h).

''(3) LIMITATIONS.—The Director shall not be required—

''(A) to obtain the approval of any other officer or employee of the United States Government with respect to the collection or analysis of any information; or

''(B) prior to publication, to obtain the approval of any other officer or employee of the United States Government with respect to the substance of any statistical technical reports or press releases lawfully prepared by the Director.

''(4) QUALIFICATIONS.—The Director—

''(A) shall have experience in statistical programs and information security; and

''(B) may not—

''(i) engage in any other employment; or

''(ii) hold any office in, or act in any capacity for, any organization, agency, or institution with which the Office makes

any contract or other arrangement under this section.

''(5) DUTIES AND FUNCTIONS.—The Director shall—

''(A) collect, survey, and analyze information concerning cybersecurity, including data related to cyber incidents, cyber crime, and any other cyber area the Director determines appropriate;

''(B) collect, survey, and analyze data that will serve as a continuous and comparable national indication of the prevalence, rates, extent, distribution, and attributes of all relevant cyber incidents, as determined by the Director, in support of national policy and decision making;

''(C) compile, collate, analyze, publish, and disseminate uniform, anonymized, aggregated national cyber data concerning any cyber area that the Director determines appropriate;

''(D) in coordination with the National Institute of Standards and Technology, the Director of National Intelligence, the Secretary of Defense, and the Attorney General, recommend national standards, metrics, and measurement criteria for the collection of cyber statistics and

for ensuring the reliability and validity of such statistics collected pursuant to this subsection;

''(E) conduct or support research relating to methods of gathering or analyzing cyber statistics and anonymized datasets;

''(F) enter into grants and cooperative agreements or contracts with public agencies, institutions of higher education, or private organizations for purposes related to this subsection;

''(G) provide appropriate anonymized, aggregated information and analysis to the President, Congress, Federal agencies, the private sector, and the general public on cyber statistics;

''(H) share information with State and local governments concerning cyber statistics; and

''(I) confer and cooperate with Federal statistical agencies as needed to carry out the purposes of this section, including by entering into cooperative data sharing agreements.

''(d) COLLECTION OF HOMELAND SECURITY CYBERSECURITY DATA.—

''(1) IDENTIFICATION.—Not later than 180 days after the date of the enactment of this section and every two years thereafter, the Director, in consultation with the Director of the Agency, shall—

''(A) identify and inventory existing sources of data and information concerning cybersecurity, including data and information concerning cyber incidents and cyber threat indicators, managed by the Department; and

''(B) among that inventory, identify such data and information relevant to the purposes of subsection (c) that can be shared with the Office.

''(2) PROCEDURES.—No later than 180 days after completion of the identification and inventorying required under paragraph (1), the Director, in consultation with the Director of the Agency and the Secretary, shall disseminate common procedures that govern how the data and information so identified and inventoried may be transmitted to the Office.

''(3) DATA REQUESTS.—The Director of the Office shall have the authority to request any data and information under paragraph (1).

''(4) REPORTING.—The Director of the Agency shall ensure that the data and information under paragraph (1) which is held by the Agency is provided upon request to the Office via the procedures described in paragraph (2), unless such data is subject to a separate reporting requirement under this section.

''(5) SUPPORT.—The Director may, in coordination with the Director of the Agency, work jointly across the Agency to improve the availability and quality of Agency cybersecurity data.

''(e) FURNISHMENT OF INFORMATION, DATA, OR REPORTS BY FEDERAL DEPARTMENTS AND AGENCIES.—

''(1) DEFINITION.—In this subsection, the term 'incident' has the meaning given that term in section 3552 of title 44, United States Code.

''(2) CONSULTATION.—The Director shall consult with the Director of the Office of Management and Budget, the Secretary, and the National Cyber Director with respect to data collection on the reporting of incidents.

''(3) REPORTING CYBERSECURITY DATA.—Not later than one year after the date of the enactment of this section and annually thereafter, the Director shall provide the Director of the Office of Manage-

ment and Budget, the Secretary, and the National Cyber Director a list of data recommended to be reported in order to develop meaningful cybersecurity statistics regarding incidents affecting Federal information systems.

''(4) ENFORCEMENT.—The Director of the Office of Management and Budget, in consultation with the Secretary and the National Cyber Director, shall annually determine which cybersecurity data recommended pursuant to paragraph (3) to require from Federal departments and agencies and use the authority under section 3553 of title 44, United States Code, to ensure such departments and agencies provide such data to the Office.

''(f) FURNISHMENT OF INFORMATION, DATA, OR REPORTS BY STATE GOVERNMENTS.—

''(1) IN GENERAL.—The Director shall request information necessary to carry out the purposes of subsection (c), including information collected through data breach reporting laws of States, from State governments.

''(2) STANDARDIZATION.—Not later than one year after the date of the enactment of this section and every two years thereafter, the Director shall publish—

''(A) a description of the information and data from State governments determined necessary to carry out the purposes of subsection (c), including information collected through data breach reporting laws of States; and

''(B) common standard requirements through which States may transmit to the Office information and data described in subparagraph (A).

''(3) GRANTS TO STATES FOR THE SUBMISSION OF INFORMATION AND DATA.—

''(A) IN GENERAL.—The Director may award grants to States to assist in collecting and transmitting to the Office information and data in accordance with the standards published under paragraph (2).

''(B) APPLICATION.—Each State that desires a grant under this paragraph shall submit an application to the Director at such time, in such manner, and accompanied by or containing such information as the Director shall require.

''(C) DATE FOR SUBMISSION.—Applications submitted under subparagraph (B) shall

be submitted during the 60-day period beginning on a date that the Director shall prescribe.

''(D) DEADLINE.—An application for a grant under this paragraph shall be approved or denied by the Director not later than 90 days after the date on which the Director receives the application.

''(E) GRANT AMOUNT.—A grant under this paragraph shall not exceed $200,000 for any single State in any one-year period.

''(F) REPORTING.—

''(i) COMPLIANCE.—

''(I) IN GENERAL.—Except as provided in subclauses (II) and (III), on and after the date that is one year after the date on which a State receives a grant under this paragraph, and every three months thereafter during the grant period, the State shall submit to the Director information specified in paragraph (2).

''(II) EXTENSIONS.—The Director may provide an extension to a State that is making good faith efforts to comply with subclause (I).

"(III) NEW DATA.—If, pursuant to paragraph (2), the Director publishes a new description of information and data determined necessary to carry out the purposes of subsection (c), a State shall include information relating to such new information and data, to the extent available to the State, in each submission under subclause (I) made by the State on or after the date that is one year after the date on which the Director so publishes such new description.

"(ii) FAILURE TO COMPLY.—If a State that receives a grant under subparagraph (B) fails to substantially comply with clause (i) of this subparagraph, the State shall repay the grant in full.

"(G) BIENNIAL REPORTS.—Not later than one year after the date of enactment of this section and every two years thereafter, the Director shall submit to Congress a report describing the applications submitted for grants under this paragraph, the award of such grants, the purposes for which the grant amounts were ex-

pended, and an assessment of the effectiveness of the awarded grants in generating relevant information and data for the Office.

''(g) FURNISHMENT OF DATA AND INFORMATION RELATED TO COVERED CLAIMS.—

''(1) IN GENERAL.—The Director shall request data and information from insurance providers and other sources about cyber incidents that lead to a covered claim.

''(2) IDENTIFICATION OF RELEVANT DATA AND INFORMATION.—Not later than 270 days after the date of the enactment of this section, the Director shall identify a list of data and information determined necessary to carry out the purposes of this section, including individual descriptions of cyber incidents that lead to a covered claim, including—

''(A) identification of the affected databases, information systems, or devices that were, or are reasonably believed to have been, accessed by an unauthorized person;

''(B) a description of the vulnerabilities, tactics, techniques, and procedures used;

''(C) any identifying information related to the malicious actors that perpetrated such cyber incidents;

''(D) documentation of cybersecurity policies put in place by the affected entities, including relevant cybersecurity controls;

''(E) a description of the network security of the affected entities during the course of such cyber incidents, including the state of implementation of commonly used cybersecurity controls;

''(F) the total amount of the claim paid for each such cyber incident and any additional information about the scope of damage of each such cyber incident; and

''(G) the industrial sectors, regions, estimated annual revenue, and number of employees of affected entities without providing any information that can reasonably be expected to identify such entities.

''(3) REPORTING.—Not later than one year after the date of the enactment of this section, the Director shall publish common standardized procedures that—

''(A) outline how data and information identified under paragraph (2) may be transmitted to the Office, with consideration for ex-

isting cyber data reporting models and frameworks; and

''(B) avoid duplicative reporting to the office in a case in which a cyber incident results in multiple claims paid, or in the case in which a cyber incident results in both a claim paid by a covered entity and either a report under a State data breach reporting law or a report submitted to the Agency under subtitle D.

''(4) IMMUNITY FROM PROCESS; PROHIBITION AGAINST ADMISSION AS EVIDENCE OR USE IN ANY PROCEEDINGS.—No officer or employee of the Federal Government, and no recipient of assistance under the provisions of this section may use or reveal any research or statistical information furnished under this section by any entity and identifiable to any specific entity for any purpose other than the purpose for which it was obtained in accordance with this subsection. Such information and copies thereof shall be immune from legal process, and may not, without the consent of the entity furnishing such information, be admitted as evidence or used for any purpose in any action, suit, or other judicial, legislative, or administrative proceedings. Data or information disclosed to the Office under this subsection

that is not otherwise available may not be used by the Federal Government or any State, local, Tribal, or territorial government to sanction or otherwise punish the entity disclosing such data or information, or the entity in which the cyber incident initially occurred.

''(5) PRESERVATION OF PRIVILEGE.—Disclosure of data or information pursuant to this subsection or by a covered entity to the Office shall not waive any otherwise applicable privilege, immunity, or protection provided by law.

''(6) PRESERVATION OF EXISTING OBLIGATIONS.—Nothing in this subsection shall modify, prevent, or abrogate any notice or notification obligations under Federal contracts, enforceable agreements with the Government, or other Federal law.

''(7) STUDY REQUIRED.—Not later than three years after the date of the enactment of this section the Director shall submit to Congress a report evaluating the Office's ability to carry out this subsection and recommending policy options to enhance the Office's capacity to collect data and information relating to cyber incidents that lead to a covered claim. The report shall, at minimum, include the following:

''(A) An evaluation of the availability to the Office of data and information identified pursuant to paragraph (2).

''(B) An evaluation of the Office's current resources and authorities to collect such data and information.

''(C) An evaluation of policy options that would facilitate the Office's access to such data and information.

''(D) An evaluation of the Office's options to collect such data and information through voluntary partnerships with private organizations formed by covered entities for the purposes of pooling actuarial data.

''(h) PROTECTION OF INFORMATION.—

''(1) IN GENERAL.—No officer or employee of the Federal Government or agent of the Federal Government may, without the consent of the individual, entity, agency, or other person who is the subject of the submission or provides the submission—

''(A) use any submission that is furnished for exclusively statistical purposes under this section for any purpose other than the statis-

tical purposes for which such submission is furnished;

''(B) make any publication or media transmittal of the data contained in a submission described in subparagraph (A) that permits information concerning individual entities or individual incidents to be reasonably inferred by either direct or indirect means; or

''(C) permit anyone other than a sworn officer, employee, agent, or contractor of the Office to examine an individual submission described in subsection (g).

''(2) PENALTY.—Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law.

''(3) EXEMPTION FROM DISCLOSURE.—Pursuant to section 552(b)(3) of title 5, United States Code, any submission collected and retained by the Agency under this section may not be disclosed to the public, unless such information has been transformed into an anonymized, aggregate form.

''(4) IMMUNITY FROM LEGAL PROCESS.—Any submission (including any data derived from the

submission) that is collected and retained by the Office, or an officer, employee, agent, or contractor of the Office, for exclusively statistical purposes under this section shall be immune from the legal process and may not, without the consent of the individual, entity, agency, or other person who is the subject of the submission or who provides the submission, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding against the person or entity that submitted the report, or on whose behalf the report was submitted.

''(5) RULE OF CONSTRUCTION.—Nothing in this subsection may be construed to provide immunity from the legal process for a submission (including any data derived from the submission) if the submission is in the possession of any person, agency, or entity other than the Office or an officer, employee, agent, or contractor of the Office, or if the submission is independently collected, retained, or produced for purposes other than the purposes of this section.

''(6) DIGITAL SECURITY.—The Agency shall ensure that reports submitted to the Office pursuant to this section, and any information contained in

such reports, are collected, stored, and protected at a minimum in accordance with the requirements for moderate impact Federal information systems, as described in Federal Information Processing Standards Publication 199, or any successor document. The Director shall consult with the Director of the Agency to ensure decisions related to information technology guarantee the protection of the confidentiality of information provided solely for statistical purposes, in accordance with subchapter III of chapter 35 of title 44, United States Code.

''(7) IMPLEMENTATION.—Chapter 35 of title 44, United States Code, shall not apply to any action to implement this section.

''(i) AUTHORIZATION OF APPROPRIATION.—There are authorized to be appropriated such sums as may be necessary to carry out this section. Such funds are authorized to remain available until expended.''.

(b) TECHNICAL AND CONFORMING AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by inserting after the item relating to section 2220D the following new item:

''Sec. 2220E. Office of Cybesecurity Statistics.''.

☒