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. 5206. SYSTEMICALLY IMPORTANT ENTITIES.

(a) IDENTIFICATION OF SYSTEMICALLY IMPORTANT ENTITIES.—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 new section:

"SEC. 2220D. PROCEDURE FOR DESIGNATION OF SYSTEMICALLY IMPORTANT ENTITIES.

''(a) ESTABLISHMENT OF CRITERIA AND PROCEDURES.—

''(1) IN GENERAL.—Not later than 12 months after the date of the enactment of this section, the Secretary, acting through the Director, in consultation with the National Cyber Director, Sector Risk Management Agencies, the Critical Infrastructure Partnership Advisory Council, and, as appropriate, other government and nongovernmental entities, shall establish criteria and procedures for identifying and designating certain entities as systemically important entities for purposes of this section.

''(2) CONSIDERATION.—In establishing the criteria for designation under paragraph (1), the Secretary shall consider the following:

''(A) The consequences that a disruption to a system, asset, or facility under an entity's control would have on one or more national critical functions.

''(B) The degree to which the entity has the capacity to engage in operational collaboration with the Agency, and the degree to which such operational collaboration would benefit national security.

''(C) The entity's role and prominence within critical supply chains or in the delivery of critical functions.

''(D) Any other factors the Secretary determines appropriate.

''(3) ELEMENTS.—The Secretary shall develop a mechanism for owners and operators of critical infrastructure to submit information to assist the Secretary in making designations under this subsection.

''(b) DESIGNATION OF SYSTEMICALLY IMPORTANT ENTITIES.—

''(1) IN GENERAL.—The Secretary, using the criteria and procedures established under subsection

(a)(1) and any supplementary information submitted under subsection (a)(3), shall designate certain entities as systemically important entities.

''(2) NOTIFICATION OF DESIGNATION STATUS.—The Secretary shall notify designees within 30 days of designation or dedesignation, with an explanation of the basis for such determination.

''(3) REGISTER.—The Secretary shall maintain and routinely update a list, or register, of such entities, with contact information.

''(4) LIMITATIONS.—

''(A) IN GENERAL.—The number of designated entities shall not exceed 200 in total.

''(B) SUNSET.—Beginning on the date that is four years after the date of the enactment of this section, the Secretary, after consultation with the Director, may increase the number of designated entities provided—

''(i) such number does not exceed 150 percent of the prior maximum;

''(ii) the Secretary publishes such new maximum number in the Federal Register; and

"(iii) such new maximum number has not been changed in the immediately preceding four years.

"(c) REDRESS.—

"(1) IN GENERAL.—Subject to paragraph (2), the Secretary shall develop a mechanism, consistent with subchapter II of chapter 5 of title 5, United States Code, for an entity notified under subsection (b)(2) to present evidence that the Secretary should reverse—

"(A) the designation of a facility, system, or asset as systemically important critical infrastructure;

"(B) the determination that a facility, system, or asset no longer constitutes systemically important critical infrastructure; or

"(C) a final judgment entered in a civil action seeking judicial review brought in accordance with paragraph (2).

"(2) APPEAL TO FEDERAL COURT.—A civil action seeking judicial review of a final agency action taken under the mechanism developed under paragraph (1) shall be filed in the United States District Court for the District of Columbia.

''(d) REPORTING FOR SYSTEMICALLY IMPORTANT ENTITIES.—

''(1) IN GENERAL.—Not later than two years after the date of the enactment of this section, the Secretary, acting through the Director, in consultation with the National Cyber Director, Sector Risk Management Agencies, the CISA Cybersecurity Advisory Committee, and relevant government and non-government entities, shall establish reporting requirements for systemically important entities.

''(2) REQUIREMENTS.—The requirements established under subsection (a) shall directly support the Department's ability to understand and prioritize mitigation of risks to national critical functions and ensure that any information obtained by a systemically important entity pursuant to this section is properly secured.

''(3) REPORTED INFORMATION.—The requirements under paragraph (2) may include obligations for systemically important entities to—

''(A) identify critical assets, systems, suppliers, technologies, software, services, processes, or other dependencies that would inform the Federal Government's understanding of the

risks to national critical functions present in the entity's supply chain;

''(B) associate specific third-party entities with the supply chain dependencies identified under subparagraph (A);

''(C) detail the supply chain risk management practices put in place by the systemically important entity, including, where applicable, any known security and assurance requirements for third-party entities under subparagraph (B); and

''(D) identify any documented security controls or risk management practices that third-party entities have enacted to ensure the continued delivery of critical services to the systemically important entity.

''(4) DUPLICATIVE REQUIREMENTS.—

''(A) IN GENERAL.—The Secretary shall coordinate with the head of any Federal agency with responsibility for regulating the security of a systemically important entity to determine whether the reporting requirements under this subsection may be fulfilled by any reporting requirement in effect on the date of the enact-

ment of this section or subsequently enacted after such date.

''(B) EXISTING REQUIRED REPORTS.—If the Secretary determines that an existing reporting requirement for a systemically important entity substantially satisfies the reporting requirements under this subsection, the Secretary shall accept such report and may not require a such entity to submit an alternate or modified report.

''(C) COORDINATION.—The Secretary shall coordinate with the head any Federal agency with responsibilities for regulating the security of a systemically important entity to eliminate any duplicate reporting or compliance requirements relating to the security or resiliency of such entities.

''(e) INTELLIGENCE SUPPORT TO SYSTEMICALLY IMPORTANT ENTITIES.—

''(1) IDENTIFICATION OF INFORMATION NEEDS.—Not later than one year after the date of the enactment of this section, the Secretary, acting through the Director, shall establish a process to solicit and compile relevant information from Sector Risk Management Agencies and any other relevant

Federal agency to inform and identify common information needs and interdependencies across systemically important entities

''(2) INTERDEPENDENCIES AND RISK IDENTIFICATION.—In establishing the process under paragraph (1), the Secretary, acting through the Director, shall incorporate methods and procedures—

''(A) to identify the types of information needed to understand interdependence of systemically important entities and areas where a nation-state adversary may target to cause widespread compromise or disruption, including—

''(i) common technologies, including hardware, software, and services, used within systemically important entities;

''(ii) critical lines of businesses, services, processes, and functions on which multiple systemically important entities are dependent;

''(iii) specific technologies, components, materials, or resources on which multiple systemically important entities are dependent; and

''(iv) Federal, State, local, Tribal, or territorial government services, functions, and processes on which multiple systemically important entities are dependent; and

''(B) to associate specific systemically important entities with the information identified under subparagraph (A),

''(3) INFORMATION NEEDS AND INDICATIONS AND WARNING.—In establishing the process under paragraph (1), the Secretary, acting through the Director, in consultation with the Director of National Intelligence, shall incorporate methods and procedures to—

''(A) provide indications and warning to systemically important entities regarding nation-state adversary cyber operations relevant to information identified under paragraph (2)(A); and

''(B) to identify information needs for the cyber defense efforts of such entities.

''(4) RECURRENT INPUT.—Not later than 30 days after the establishment of the process under paragraph (1) and no less often than biennially thereafter, the Secretary, acting through the Direc-

tor, shall solicit information from systemically important entities utilizing such process.

''(5) INTELLIGENCE SHARING.—

''(A) IN GENERAL.—Not later than five days after discovery of information that indicates a credible threat to an identifiable systemically important entity, the Director of National Intelligence, in coordination with the Secretary, shall share the appropriate intelligence information with such entity.

''(B) EMERGENCY NOTIFICATION.—The Director of National Intelligence, in coordination with the Secretary, shall share any intelligence information related to a systemically important entity with such entity not later than 24 hours after the Director of National Intelligence determines that such information indicates an imminent threat—

''(i) to such entity, or to a system, asset, or facility such entity owns or operates; or

''(ii) to national security, economic security, or public health and safety relevant to such entity.

''(C) NATIONAL SECURITY EXEMPTIONS.—Notwithstanding subparagraphs (A) or (B), the Director of National Intelligence may withhold intelligence information pertaining to a systemically important entity if the Director of National Intelligence, with the concurrence of the Secretary and the Director, determines that withholding such information is in the national security interest of the United States.

''(D) REPORT TO CONGRESS.—Not later than three years after the date of the enactment of this section and annually thereafter, the Secretary, in coordination with the National Cyber Director and the Director of National Intelligence, shall submit to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Government Affairs of the Senate, the Permanent Select Committee on Intelligence of the House of Representatives, and the Select Committee on Intelligence of the Senate, a report that—

''(i) provides an overview of the intelligence information shared with systemically important entities; and

''(ii) evaluates the relevance and success of the classified, actionable information the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)) provided to systemically important entities.

''(E) INTELLIGENCE SHARING.—Notwithstanding any other provision of law, information or intelligence shared with systemically important entities under the processes established under this subsection shall not constitute favoring one private entity over another.

''(f) PRIORITIZATION.—In allocating Department resources, the Secretary shall prioritize systemically important entities in the provision of voluntary services, and encourage participation in programs to provide technical assistance in the form of continuous monitoring and detection of cybersecurity risks.

''(g) INCIDENT RESPONSE.—In the event that a systemically important entity experiences a serious cyber incident, the Secretary shall—

''(1) promptly establish contact with such entity to acknowledge receipt of notification, obtain additional information regarding such incident, and as-

certain the need for incident response or technical assistance;

''(2) maintain routine or continuous contact with such entity to monitor developments related to such incident;

''(3) assist in incident response, mitigation, and recovery efforts;

''(4) ascertain evolving needs of such entity; and

''(5) prioritize voluntary incident response and technical assistance for such covered entity.

''(h) OPERATIONAL COLLABORATION WITH SYSTEMICALLY IMPORTANT ENTITIES.—The head of the office for joint cyber planning established pursuant to section 2216, in carrying out the responsibilities of such office with respect to relevant cyber defense planning, joint cyber operations, cybersecurity exercises, and information-sharing practices, shall, to the extent practicable, prioritize the involvement of systemically important entities.

''(i) EMERGENCY PLANNING.—In partnership with systemically important entities, the Secretary, in coordination with the Director, the heads of Sector Risk Management Agencies, and the heads of other Federal agencies with responsibilities for regulating critical infrastructure,

shall regularly exercise response, recovery, and restoration plans to—

''(1) assess performance and improve the capabilities and procedures of government and systemically important entities to respond to a major cyber incident; and

''(2) clarify specific roles, responsibilities, and authorities of government and systemically important entities when responding to such an incident.

''(j) INTERAGENCY COUNCIL FOR CRITICAL INFRASTRUCTURE CYBERSECURITY COORDINATION.—

''(1) INTERAGENCY COUNCIL FOR CRITICAL INFRASTRUCTURE CYBERSECURITY COORDINATION.—There is established an Interagency Council for Critical Infrastructure Cybersecurity Coordination (in this section referred to as the 'Council').

''(2) CHAIRS.—The Council shall be co-chaired by—

''(A) the Secretary, acting through the Director; and

''(B) the National Cyber Director.

''(3) MEMBERSHIP.—The Council shall be comprised of representatives from the following:

''(A) Appropriate Federal departments and agencies, including independent regulatory

agencies responsible for regulating the security of critical infrastructure, as determined by the Secretary and National Cyber Director.

''(B) Sector Risk Management Agencies.

''(C) The National Institute of Standards and Technology.

''(4) FUNCTIONS.—The Council shall be responsible for the following:

''(A) Reviewing existing regulatory authorities that could be utilized to strengthen cybersecurity for critical infrastructure, as well as potential forthcoming regulatory requirements under consideration, and coordinating to ensure that any new or existing regulations are streamlined and harmonized to the extent practicable, consistent with the principles described in paragraph (5).

''(B) Developing cross-sector and sector-specific cybersecurity performance goals that serve as clear guidance for critical infrastructure owners and operators about the cybersecurity practices and postures that the American people can trust and should expect for essential services.

''(C) Facilitating information sharing and, where applicable, coordination on the development of cybersecurity policy, rulemaking, examinations, reporting requirements, enforcement actions, and information sharing practices.

''(D) Recommending to members of the council general supervisory priorities and principles reflecting the outcome of discussions among such members.

''(E) Identifying gaps in regulation that could invite cybersecurity risks to critical infrastructure, and as appropriate, developing legislative proposals to resolve such regulatory gaps.

''(F) Providing a forum for discussion and analysis of emerging cybersecurity developments and cybersecurity regulatory issues.

''(5) PRINCIPLES.—In carrying out the activities under paragraph (4), the Council shall seek to harmonize regulations in a way that—

''(A) avoids duplicative, overlapping, overly burdensome, or conflicting regulatory requirements that do not effectively or efficiently serve the interests of national security, economic security, or public health and safety;

''(B) is consistent with national cyber policy and strategy, including the National Cyber Strategy;

''(C) recognizes and prioritizes the need for the Cybersecurity and Infrastructure Security Agency, as the lead coordinator for the security and resilience of critical infrastructure across all sectors, to have visibility regarding cybersecurity threats and security vulnerabilities across sectors, and leverages regulatory authorities in a manner that supports such cross-sector visibility and coordination, to the extent practicable; and

''(D) recognizes and accounts for the variation within and among critical infrastructure sectors with respect to the level of cybersecurity maturity, the nature of the infrastructure and assets, resources available to deploy security measures, and other factors.

''(6) LEVERAGING EXISTING COORDINATING BODIES.—The Council shall, as appropriate in the determination of the Co-Chairs, carry out its work in coordination with critical infrastructure stakeholders, including sector coordinating councils and information sharing and analysis organizations, and

the Cyber Incident Reporting Council established pursuant to section 2246.

''(7) CONGRESSIONAL OVERSIGHT.—Not later than one year after the date of the enactment of this section and annually thereafter, the Council shall report to the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Government Affairs of the Senate, and other relevant congressional committees, on the activities of the Council, including efforts to harmonize regulatory requirements, and close regulatory gaps, together with legislative proposals, as appropriate.

''(k) STUDY ON PERFORMANCE GOALS FOR SYSTEMICALLY IMPORTANT ENTITIES.—

''(1) IN GENERAL.—The Council shall conduct a study to develop policy options and recommendations regarding the development of risk-based cybersecurity performance benchmarks that, if met, would establish a common minimum level of cybersecurity for systemically important entities.

''(2) AREAS OF INTEREST.—The study required under paragraph (1) shall evaluate how the performance benchmarks referred to in such paragraph can be—

''(A) flexible, nonprescriptive, risk-based, and outcome-focused;

''(B) designed to improve resilience and address cybersecurity threats and security vulnerabilities while also providing an appropriate amount of discretion to operators in deciding which specific technologies or solutions to deploy;

''(C) applicable and appropriate across critical infrastructure sectors, but also adaptable and augmentable to develop tailored, sector-specific cybersecurity performance goals; and

''(D) reflective of existing industry best practices, standards, and guidelines to the greatest extent possible.

''(l) DEFINITIONS.—In this section:

''(1) SYSTEMICALLY IMPORTANT ENTITY.—The term 'systemically important entity' means a critical infrastructure entity the Secretary has designated as a systemically important entity pursuant to subsection (b).

''(2) DIRECTOR.—The term 'Director' means the Director of the Cybersecurity and Infrastructure Security Agency.

''(3) SECTOR RISK MANAGEMENT AGENCY.—The term 'Sector Risk Management Agency' has the meaning given such term is section 2201.

''(4) NATIONAL CRITICAL FUNCTIONS.—The term 'national critical functions' means functions of government or private sector so vital to the United States that the disruption, corruption, or dysfunction of such functions would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.''.

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

''Sec. 2220D. Procedure for designation of covered systemically important entities.''.