AMENDMENT TO RULES COMM. PRINT 116–57
OFFERED BY MR. RICHMOND OF LOUISIANA

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

SEC. 16___. CRITICAL INFRASTRUCTURE CYBER INCIDENT REPORTING PROCEDURES.

(a) IN GENERAL.—Not later than one year after the date of enactment of this Act, the Secretary, acting through the Director, and in consultation with Sector Risk Management Agencies and other appropriate Federal departments, shall, after notice and an opportunity for comment, establish requirements and a process for covered critical infrastructure entities to report a covered cybersecurity incident to the national cybersecurity and communications integration center of the Department of Homeland Security, in furtherance of its mission with respect to cybersecurity risks as set forth in section 2209.

(b) PROCEDURES.—The cybersecurity incident reporting requirements and process described in subsection (a) shall, at a minimum, include—

(1) a definition of covered critical infrastructure entities that are required to comply with the report-

ing requirements of this section, based on threshold criteria related to—

(A) the likelihood that such entity may be targeted by a malicious cyber actor, including a foreign country;

(B) consequences that disruption to or compromise of such entity could cause to national security, economic security, or public health and safety; and

(C) maturity of security operations in detecting, investigating, and mitigating a cybersecurity incident;

(2) criteria for the types and thresholds for a covered cybersecurity incident to be reported under this section, including the sophistication or novelty of the cyber attack, the type, volume, and sensitivity of the data at issue, and the number of individuals affected or potentially affected by a cybersecurity incident, subject to the limitations described in subsection (c); and

(3) procedures to comply with reporting requirements pursuant to subsection (c).

(c) CYBERSECURITY INCIDENT REPORTING REQUIREMENTS FOR COVERED CRITICAL INFRASTRUCTURE ENTITIES.—

(1) IN GENERAL.—A covered critical infrastructure entity, as defined by the Director pursuant to subsection (b),meets the requirements of this paragraph if, upon becoming aware that a covered cybersecurity incident, including an incident involving ransomware, social engineering, malware, or unauthorized access, has occurred involving any critical infrastructure system or subsystem of the critical infrastructure, the entity—

(A) promptly reports such incident to the national cybersecurity and communications integration center, consistent with such requirements and process, as soon as practicable (but in no case later than 72 hours after the entity first becomes aware that the incident occurred); and

(B) provides all appropriate updates to any report submitted under subparagraph (A).

(2) CONTENTS OF REPORT.—Each report submitted under subparagraph (A) of paragraph (1) shall contain such information as the Director prescribes in the reporting procedures issued under subsection (a), including the following information with respect to any cybersecurity incident covered by the report:

(A) The date, time, and time zone when the cybersecurity incident began, if known.

(B) The date, time, and time zone when the cybersecurity incident was detected.

(C) The date, time, and duration of the cybersecurity incident.

(D) The circumstances of the cybersecurity incident, including the specific critical infrastructure systems or subsystems believed to have been accessed and information acquired, if any, as well as any interdependent systems that suffered damage, disruption, or were otherwise impacted by the incident.

(E) Any planned and implemented technical measures to respond to and recover from the incident.

(F) In the case of any report which is an update to a prior report, any additional material information relating to the incident, including technical data, as it becomes available.

(d) EFFECT OF OTHER REPORTING.—A covered critical infrastructure entity shall not be considered to have satisfied the reporting requirements set forth in subsection (c)(1) by reporting information required pursuant to subsection (c)(2) related to a covered cybersecurity incident

to any person, agency or organization, including a law enforcement agency, other than to the Director using the incident reporting procedures establish by the national cybersecurity and communications integration center using the incident reporting procedures established by the Director pursuant to subsection (a). (e) DISCLOSURE, RETENTION, AND USE.—

(1) AUTHORIZED ACTIVITIES.—Covered cybersecurity incidents and related reporting information provided to the Director pursuant to this section may not be disclosed to, retained by, or? used by, consistent with otherwise applicable provisions of Federal law, any Federal agency or department, or any component, officer, employee, or agent of the Federal Government, except if the Director determines such disclosure, retention, or use is necessary for—

(A) the purpose of identifying—

(i) a cybersecurity threat as such term is defined insection 102(5) of the Cybersecurity Act of 2015 (contained in division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501)), including the source of such cybersecurity threat; or

(ii) a security vulnerability;

(B) the purpose of responding to, or otherwise preventing or mitigating, a specific threat of death, serious bodily harm, or serious economic harm, including a terrorist act or a use of a weapon of mass destruction;

(C) the purpose of responding to, investigating, prosecuting, or otherwise preventing or mitigating, a serious threat to a minor, including sexual exploitation and threats to physical safety; or

(D) the purpose of preventing, investigating, disrupting, or prosecuting an offense arising out of a threat described in subparagraphs (B)-(C) (3) or any of the offenses listed in—

(i) sections 1028 through 1030 of title 18, United States Code (relating to fraud and identity theft);

(ii) chapter 37 of such title (relating to espionage and censorship); and

(iii) chapter 90 of such title (relating to protection of trade secrets).

(2) EXCEPTION.—The Director may enter into an agreement with a federally funded research and

development center or other research institution to provide information in an anonymized manner for the purpose of aggregating and analyzing cybersecurity incident data and other reported information for the limited purpose of better understanding the cyber threat landscape, subject to appropriate protections for information and removal of any unnecessary personal or identifying information.

(3) PRIVACY AND CIVIL LIBERTIES.—Covered cybersecurity incidents and related reporting information provided to the Director pursuant to this section shall be retained, used, and disseminated, where permissible and appropriate, by the Federal Government—

(A) in a manner that protects from unauthorized use or disclosure any information reported under this section that may contain—

(i) personal information of a specific individual; or

(ii) information that identifies a specific individual; and

(B) in a manner that protects the confidentiality of information reported under this section containing—

(i) personal information of a specific individual; or

(ii) information that identifies a specific individual.

(4) FEDERAL REGULATORY AUTHORITY.—Information regarding a covered cybersecurity incident and related reporting information provided to the Director pursuant to this section may not be used by any Federal, State, Tribal, or local government to regulate, including through an enforcement action, the lawful activities of any non-Federal entity.

(f) LIMITATION.—The Director may not set criteria or develop procedures pursuant to this Act that require a covered critical infrastructure entity, identified pursuant to subsection (b)(1), to report on any cybersecurity incident unless such incident—

(1) causes a loss in the confidentiality, integrity, or availability of proprietary, sensitive, or personal information;

(2) results in a disruption or otherwise inhibits the ability of an entity to deliver services or conduct its primary business activity; or

(3) was carried out by a foreign country, or where there is reason to believe a foreign country was involved in such incident.

(g) DEFINITIONS.—In this section:

(1) COVERED CRITICAL INFRASTRUCTURE ENTITY.—The term ''covered critical infrastructure entity'' is an entity thatowns, operates, supports, or maintains critical infrastructure which meets the definition set forth by the Director pursuant to subsection (b)(1).

(2) COVERED CYBERSECURITY INCIDENT.—The term ''covered cybersecurity incident'' means a cybersecurity incident experienced by a covered critical infrastructure entity that meets the definition and criteria set forth by the Director in the procedures prescribed pursuant to subsection (b)(2), subject to the limitations in subsection (f).) that involve, at a minimum, an incident that—

(3) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given that term in section 2(4) of the Homeland Security Act of 2002 (Public Law 107–196; 6 U.S.C. 101(4)).

(4) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given that term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(5) DEPARTMENT.—The term ''Department'' means the Department of Homeland Security.

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

(7) NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER.—The term ''national cybersecurity and communications integration center'' or ''Center'' means the national cybersecurity and communications integration center described in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(8) SECRETARY.—The term ''Secretary'' means the Secretary of Homeland Security.

(9) SECTOR SPECIFIC AGENCY.—The term ''Sector Specific Agency'' has the meaning given that term in section 2201(5) of the Homeland Security Act of 2002 (6 U.S.C. 651(5)).

☒