AMENDMENT TO RULES COMM. PRINT 117–13
OFFERED BY MS. CLARKE OF NEW YORK

Add at the end of subtitle D of title XV of division A the following:

SEC. 15___. CYBERSENTRY PROGRAM OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) IN GENERAL.—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. 2220A. CYBERSENTRY PROGRAM.

''(a) ESTABLISHMENT.—The Director shall establish and maintain in the Agency a program, to be known as 'CyberSentry', to provide continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions, upon request and subject to the consent of such owner or operator.

''(b) ACTIVITIES.—The Director, through CyberSentry, shall—

''(1) enter into strategic partnerships with critical infrastructure owners and operators that, in the determination of the Director and subject to the

availability of resources, own or operate regionally or nationally significant industrial control systems that support national critical functions, in order to provide technical assistance in the form of continuous monitoring of industrial control systems and the information systems that support such systems and detection of cybersecurity risks to such industrial control systems and other cybersecurity services, as appropriate, based on and subject to the agreement and consent of such owner or operator;

''(2) leverage sensitive or classified intelligence about cybersecurity risks regarding particular sectors, particular adversaries, and trends in tactics, techniques, and procedures to advise critical infrastructure owners and operators regarding mitigation measures and share information as appropriate;

''(3) identify cybersecurity risks in the information technology and information systems that support industrial control systems which could be exploited by adversaries attempting to gain access to such industrial control systems, and work with owners and operators to remediate such vulnerabilities;

''(4) produce aggregated, anonymized analytic products, based on threat hunting and continuous monitoring and detection activities and partnerships,

with findings and recommendations that can be disseminated to critical infrastructure owners and operators; and

''(5) support activities authorized in accordance with section 1501 of the National Defense Authorization Act for Fiscal Year 2022.

''(c) PRIVACY REVIEW.—Not later than 180 days after the date of enactment of this Act, the Privacy Officer of the Agency under section 2202(h) shall—

''(1) review the policies, guidelines, and activities of CyberSentry for compliance with all applicable privacy laws, including such laws governing the acquisition, interception, retention, use, and disclosure of communities; and

''(2) submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a report certifying compliance with all applicable privacy laws as referred to in paragraph (1), or identifying any instances of noncompliance with such privacy laws.

''(d) REPORT TO CONGRESS.—Not later than one year after the date of the enactment of this Act, the Director shall provide to the Committee on Homeland Security of the House of Representatives and the Committee on

Homeland Security and Governmental Affairs of the Senate a briefing and written report on implementation of this section.

''(e) SAVINGS.—Nothing in this section may be construed to permit the Federal Government to gain access to information of a remote computing service provider to the public or an electronic service provider to the public, the disclosure of which is not permitted under section 2702 of title 18, United States Code.

''(f) DEFINITIONS.—In this section:

''(1) CYBERSECURITY RISK.—The term 'cybersecurity risk' has the meaning given such term in section 2209(a).

''(2) INDUSTRIAL CONTROL SYSTEM.—The term 'industrial control system' means an information system used to monitor and/or control industrial processes such as manufacturing, product handling, production, and distribution, including supervisory control and data acquisition (SCADA) systems used to monitor and/or control geographically dispersed assets, distributed control systems (DCSs), Human-Machine Interfaces (HMIs), and programmable logic controllers that control localized processes.

''(3) INFORMATION SYSTEM.—The term 'information system' has the meaning given such term in

section 102 of the Cybersecurity Act of 2015 (enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113; 6 U.S.C. 1501(9)).''.

(b) RESPONSIBILITIES OF THE CISA DIRECTOR RELATING TO INDUSTRIAL CONTROL SYSTEMS THAT SUPPORT NATIONAL CRITICAL FUNCTIONS.—

(1) IN GENERAL.—Subsection (c) of section 2202 of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended—

(A) in paragraph (11), by striking ''and'' after the semicolon;

(B) in the first paragraph (12) (relating to appointment of a Cybersecurity State Coordinator) by striking ''as described in section 2215; and'' and inserting ''as described in section 2217;'';

(C) by redesignating the second paragraph (12) (relating to the .gov internet domain) as paragraph (13);

(D) in such redesignated paragraph (13), by striking ''and'' after the semicolon;

(E) by inserting after such redesignated paragraph (13) the following new paragraph:

''(14) maintain voluntary partnerships with critical infrastructure entities that own or operate industrial control systems that support national critical functions, which may include, upon request and subject to the consent of the owner or operator, providing technical assistance in the form of continuous monitoring and detection of cybersecurity risks (as such term is defined in section 2209(a)) in furtherance of section 2220A; and''; and

(F) by redesignating the third paragraph (12) (relating to carrying out such other duties and responsibilities) as paragraph (15).

(2) CONTINUOUS MONITORING AND DETECTION.—Section 2209(c)(6) of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended by inserting '', which may take the form of continuous monitoring and detection of cybersecurity risks to critical infrastructure entities that own or operate industrial control systems that support national critical functions'' after ''mitigation, and remediation''.

(c) TITLE XXII TECHNICAL AND CLERICAL AMENDMENTS.—

(1) TECHNICAL AMENDMENTS.—

(A) HOMELAND SECURITY ACT OF 2002.—Subtitle A of title XXII of the Homeland Secu-

rity Act of 2002 (6 U.S.C. 651 et seq.) is amended—

(i) in the first section 2215 (6 U.S.C. 665; relating to the duties and authorities relating to .gov internet domain), by amending the section enumerator and heading to read as follows:

"SEC. 2215. DUTIES AND AUTHORITIES RELATING TO .GOV INTERNET DOMAIN.";

(ii) in the second section 2215 (6 U.S.C. 665b; relating to the joint cyber planning office), by amending the section enumerator and heading to read as follows:

"SEC. 2216. JOINT CYBER PLANNING OFFICE.";

(iii) in the third section 2215 (6 U.S.C. 665c; relating to the Cybersecurity State Coordinator), by amending the section enumerator and heading to read as follows:

"SEC. 2217. CYBERSECURITY STATE COORDINATOR.";

(iv) in the fourth section 2215 (6 U.S.C. 665d; relating to Sector Risk Management Agencies), by amending the section enumerator and heading to read as follows:

"SEC. 2218. SECTOR RISK MANAGEMENT AGENCIES.";

(v) in section 2216 (6 U.S.C. 665e; relating to the Cybersecurity Advisory Committee), by amending the section enumerator and heading to read as follows:

"SEC. 2219. CYBERSECURITY ADVISORY COMMITTEE."; and

(vi) in section 2217 (6 U.S.C. 665f; relating to Cybersecurity Education and Training Programs), by amending the section enumerator and heading to read as follows:

"SEC. 2220. CYBERSECURITY EDUCATION AND TRAINING PROGRAMS.".

(B) CONSOLIDATED APPROPRIATIONS ACT, 2021.—Paragraph (1) of section 904(b) of division U of the Consolidated Appropriations Act, 2021 (Public Law 116–260) is amended, in the matter preceding subparagraph (A), by inserting ''of 2002'' after ''Homeland Security Act''.

(2) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Homeland Security Act of 2002 is amended by striking the items relating to sections 2214 through 2217 and inserting the following new items:

''Sec. 2214. National Asset Database.
''Sec. 2215. Duties and authorities relating to .gov internet domain.
''Sec. 2216. Joint cyber planning office.