AMENDMENT TO RULES COMM. PRINT 116–57
OFFERED BY MS. SLOTKIN OF MICHIGAN

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

SEC. 16___. BIENNIAL NATIONAL CYBER EXERCISE.

(a) REQUIREMENT.—Not later than December 31, 2023, and not less frequently than once every two years thereafter until a date that is not less than 10 years after the date of enactment of this Act, the Secretary, in consultation with the Secretary of Defense, shall conduct an exercise to test the resilience, response, and recovery of the United States in the case of a significant cyber attack impacting critical infrastructure.

(b) PLANNING AND PREPARATION.—Each exercise under subsection (a) shall be coordinated through the Joint Cyber Planning Office of the Cybersecurity and Infrastructure Security Planning Agency and prepared by expert operational planners from the Department of Homeland Security, in coordination with the Department of Defense, the Federal Bureau of Investigation, and the appropriate intelligence community elements, as identified by the Director of National Intelligence.

(c) PARTICIPANTS.—

(1) FEDERAL GOVERNMENT PARTICIPANTS.—The following shall participate in each exercise under subsection (a):

(A) Relevant interagency partners, as determined by the Secretary, including relevant interagency partners from—

(i) law enforcement agencies; and

(ii) the intelligence community.

(B) Senior leader representatives from sector-specific agencies, as determined by the Secretary.

(2) STATE AND LOCAL GOVERNMENTS.—The Secretary shall invite representatives from State, local, and Tribal governments to participate the exercises under subsection (a) if the Secretary determines such participation to be appropriate.

(3) PRIVATE SECTOR.—Depending on the nature of an exercise being conducted under subsection (a), the Secretary, in consultation with the senior leader representative of the sector-specific agencies participating in such exercise pursuant to paragraph (1)(A)(ii), shall invite the following individuals to participate:

(A) Representatives from private entities.

(B) Other individuals that the Secretary determines.

(4) INTERNATIONAL PARTNERS.—Depending on the nature of an exercise being conducted under subsection (a), the Secretary may, in consultation with the Secretary of Defense and the Secretary of State, invite allies and partners of the United States to participate in such exercise.

(d) OBSERVERS.—The Secretary shall invite appropriately cleared representatives from the executive and legislative branches of the Federal Government to observe an exercise under subsection (a).

(e) ELEMENTS.—Each exercise under subsection (a) shall include the following elements:

(1) Exercising the orchestration of cybersecurity response and the provision of cyber support to Federal, State, local, and Tribal governments and private entities, including the exercise of the command and control and deconfliction of operational responses through the National Security Council, interagency coordinating processes and response groups, and each participating department and agency of the Federal Government.

(2) Testing of the information-sharing needs and capabilities of exercise participants.

(3) Testing of the relevant policy, guidance, and doctrine, including the National Cyber Incident Response Plan of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security.

(4) Test the coordination between Federal, State, local, and Tribal governments and private entities.

(5) Exercising the integration of operational capabilities of the Department of Homeland Security, the Cyber National Mission Force, Federal law enforcement, and the intelligence community.

(6) Test relevant information sharing and operational agreements.

(7) Exercising integrated operations, mutual support, and shared situational awareness of the cybersecurity operations centers of the Federal Government, including the following:

(A) The Cybersecurity and Infrastructure Security Agency.

(B) The Cyber Threat Operations Center of the National Security Agency.

(C) The Joint Operations Center of United States Cyber Command.

(D) The Cyber Threat Intelligence Integration Center of the Office of the Director of National Intelligence.

(E) The National Cyber Investigative Joint Task Force of the Federal Bureau of Investigation.

(F) The Defense Cyber Crime Center of the Department of Defense.

(G) The Intelligence Community Security Coordination Center of the Office of the Director of National Intelligence.

(f) BRIEFING.—

(1) IN GENERAL.—Not later than 180 days after the date on which each exercise under subsection (a) is conducted, the President shall submit to the appropriate congressional committees a briefing on the participation of the Federal Government participants in each such exercise.

(2) CONTENTS.—Each briefing required under paragraph (1) shall include the following:

(A) An assessment of the decision and response gaps observed in the national level response.

(B) Proposed recommendations to improve the resilience, response, and recovery in the

case of a significant cyber attack impacting critical infrastructure.

(C) Plans to implement the recommendations described in subparagraph (B).

(D) Specific timelines for the implementation of such plans.

(g) REPEAL.—Subsection (b) of section 1648 of the National Defense Authorization Act for Fiscal Year 2016 (Public Law 114–92; 129 Stat. 1119) is repealed.

(h) NATIONAL CYBER EXERCISE PROGRAM.—

(1) IN GENERAL.—Not later than 180 days after the date of the enactment of this section, the Director, in consultation with appropriate representatives from sector-specific agencies, the cybersecurity research community, and Sector Coordinating Councils, shall carry out the National Cyber Exercise Program (referred to in this section as the ''Exercise Program'') to evaluate the National Cyber Incident Response Plan, and other related plans and strategies.

(2) REQUIREMENTS.—

(A) IN GENERAL.—The Exercise Program shall be—

(i) as realistic as practicable, based on current risk assessments, including credible threats, vulnerabilities, and consequences;

(ii) designed, as practicable, to simulate the partial or complete incapacitation of a State, local, or tribal government, or related critical infrastructure, resulting from a cyber incident;

(iii) carried out, as appropriate, with a minimum degree of notice to involved parties regarding the timing and details of such exercises, consistent with safety considerations;

(iv) designed to provide for the systematic evaluation of cyber readiness and enhance operational understanding of the cyber incident response system and relevant information sharing agreements; and

(v) designed to promptly develop after-action reports and plans that can be quickly incorporating lessons learned into future operations.

(B) MODEL EXERCISE SELECTION.—The Exercise Program shall include a selection of model exercises that State, local, and Tribal

governments can readily adapt for use and aid such governments with the design, implementation, and evaluation of exercises that—

(i) conform to the requirements under subparagraph (A);

(ii) are consistent with any applicable State, local, or Tribal strategy or plan; and

(iii) provide for systematic evaluation of readiness.

(i) DEFINITIONS.—In this section:

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

(A) the Committee on Armed Services of the Senate;

(B) the Committee on Armed Services of the House of Representatives;

(C) the Committee on Homeland Security and Governmental Affairs of the Senate; and

(D) the Committee on Homeland Security of the House of Representatives.

(2) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given such term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(3) INTELLIGENCE COMMUNITY.—The term ''intelligence community'' has the meaning given such term in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)).

(4) PRIVATE ENTITY.—The term ''private entity'' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

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

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

(7) STATE.—The term ''State'' means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, the Northern Mariana Islands, the United States Virgin Islands, Guam, American Samoa, and any other territory or possession of the United States.