AMENDMENT TO
RULES COMMITTEE PRINT 118–10
OFFERED BY MR. GIMENEZ OF FLORIDA

At the end of subtitle C of title XV, insert the following new section:

SEC. 15___. PORT INFRASTRUCTURE CYBERSECURITY REVIEW.

(a) REVIEW.—Not later than 240 days after the date of the enactment of this Act, the Secretary of Homeland Security, acting through the Commandant of the United States Coast Guard, in coordination with the Secretary of Defense and the Director of the Cybersecurity and Infrastructure Security Agency, shall—

(1) conduct a security risk assessment to improve the cybersecurity of each information and operational technology system used or operated by each covered strategic seaport; and

(2) develop recommendations to address any risks identified.

(b) ELEMENTS.—The security risk assessment under subsection (a)(1) shall include, with respect to each covered strategic seaport, the following:

(1) An assessment of any risks or threats posed by cybersecurity vulnerabilities of the information and operational technology systems used or operated by each covered strategic seaport, including all covered port infrastructure equipment that is manufactured, controlled or designed by a covered foreign adversary or a covered foreign entity.

(2) An assessment of whether there are any other vulnerabilities in the information and operational technology systems used or operated by each covered strategic seaport or covered port infrastructure equipment.

(3) An assessment of necessary improvements to such systems or equipment that would be needed to meet, directly or indirectly, national security and defense readiness requirements.

(4) An assessment of the risk that such identified vulnerabilities present to the successful execution of the operational or contingency plans of the Department of Defense and to the distribution of goods and services across the United States necessary for the reliable functioning of the United States economy.

(c) CONSULTATION.—The Secretary of Homeland Security shall conduct the security risk assessment under

subsection (a)(1) and develop the report under subsection (d) in consultation with the Secretary of Defense, the Secretary of Transportation, and the Area Maritime Security Advisory Committees established under section 70112(b) of title 46, United States Code.

(d) REPORT TO CONGRESS.—

(1) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary of Homeland Security, in coordination with the Secretary of Defense, shall submit to the appropriate congressional committees a report containing—

(A) a list of tools, techniques, and procedures used to test each electronic system;

(B) a list of maritime and transportation operational technologies examined;

(C) a list of stakeholders involved in the assessments;

(D) critical and high-risk cybersecurity vulnerabilities posed by existing or newly constructed ship-to-shore cranes manufactured, in whole or in part, by a covered foreign adversary or a covered foreign entity that is in use at United States covered strategic seaports;

(E) critical and high-risk cybersecurity vulnerabilities posed by existing or newly pur-

chased software, hardware, or cloud architecture designed or manufactured in whole or in part by a covered foreign adversary or a covered foreign entity that is in use at each covered strategic seaport;

(F) a prioritized list of cybersecurity vulnerabilities discovered in each covered strategic seaport that are essential for mobilization or contingency responses of the Armed Forces, including Military Ocean Terminals;

(G) a description of any gaps in authority or jurisdiction at the intersection of United States military property and civilian critical infrastructure; and

(H) risk-prioritized recommendations to mitigate threats to the defense readiness, national security, and continuity of the economy of the United States through enhanced cybersecurity at each covered strategic seaport and surrounding critical infrastructure.

(2) FORM.—The report required under paragraph (1) shall be submitted in unclassified form, but may include a classified annex.

(e) PROHIBITION.—Notwithstanding any other provision of law, no covered port infrastructure equipment for

which a contract is entered into after the date that is five years after the date of the enactment of this Act may be operated at any covered strategic seaport.

(f) DEFINITIONS.—In this section:

(1) The term ''appropriate congressional committees'' means—

(A) the Committee on Homeland Security, the Committee on Transportation and Infrastructure, the Committee on Armed Services, and the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party of the House of Representatives; and

(B) the Committee on Homeland Security and Governmental Affairs, the Committee on Commerce, Science, and Transportation, and the Committee on Armed Services of the Senate.

(2) The term ''continuity of the economy'' means the distribution of goods and services across the United States necessary for the reliable functioning of the United States economy during a significant event, through key channels of interstate commerce, including—

(A) bulk power and electric transmission systems;

(B) national and international financial systems, including wholesale payments, stocks, and currency exchanges;

(C) national and international communications networks, data-hosting services, and cloud services;

(D) interstate oil and natural gas pipelines; and

(E) mechanisms for the interstate and international trade and distribution of materials, food, and medical supplies, including road, rail, air, and maritime shipping.

(3) The term ''covered foreign adversary'' means—

(A) any foreign government or other foreign person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of United States persons; and

(B) any foreign country or foreign government identified as a strategic competitor in the

National Defense Strategy issued by the Secretary of Defense on October 27, 2022.

(4) The term ''covered foreign entity'' means any business entity—

(A) that is subject, directly or indirectly through any chain of ownership, to the jurisdiction, direction, or control of a covered foreign adversary; or

(B) in which any combination of entities subject, directly or indirectly through any chain of ownership, to the jurisdiction, direction, or control of a covered foreign adversary owns more than 20 percent of the outstanding voting stock or shares of the company.

(5) The term ''covered port infrastructure equipment'' means any operational technology, equipment, software, hardware, or cloud architecture in a covered strategic seaport that sends or receives any signal and is manufactured, controlled, or designed, in whole or in part, by a covered foreign entity.

(6) The term ''covered strategic seaport'' means a United States seaport—

(A) that is a strategic seaport, as such term is defined in section 3505(a) of the Na-

tional Defense Authorization Act for Fiscal Year 2014 (Public Law 113–66; 46 USC 50302 note); or

(B) that is determined by the Secretary of Homeland Security, in coordination with the Secretary of Defense, to be essential to the military readiness, national security, and continuity of the economy of the United States.

(7) The term ''significant event'' means an event that causes severe degradation to economic activity in the United States and that is—

(A) the result of a cyber attack; or

(B) a natural disaster or human-caused security incident.

☒