AMENDMENT TO
RULES COMMITTEE PRINT 119–33
OFFERED BY MRS. HOUCHIN OF INDIANA

At the end of subtitle B of title II, add the following:

SEC. 2_____. SECURE ARTIFICIAL INTELLIGENCE DATA CENTER DEMONSTRATION PROGRAM.

(a) DEMONSTRATION PROGRAM.—The Secretary of Defense shall, acting through the Under Secretary of Defense for Research and Engineering and in consultation with the Director of the National Security Agency and the head of the Center for Artificial Intelligence Standards and Innovation at the Department of Commerce, carry out a program to construct, prototype, and perform testing and evaluation on highly secure data centers, and to assess security requirements for such facilities, focused on—

(1) resisting attacks by nation-state adversaries;

(2) securing the confidentiality, integrity, and availability of artificial intelligence models and inference pipelines; and

(3) assessing whether existing security frameworks are sufficient to protect artificial intelligence capabilities supporting classified workloads.

(b) FOCUS.—The program required by subsection (a) shall be focused on—

(1) prototyping technologies and security controls needed to protect artificial intelligence data centers from attacks by nation-state adversaries;

(2) protecting model weights and other sensitive assets from theft, sabotage, or unauthorized access;

(3) assessing physical security, cybersecurity, supply chain, insider threat, and incident response requirements for such facilities;

(4) prototyping secure inference-only clusters or devices designed to prevent unauthorized model weight extraction or modification, including mechanisms to securely or cryptographically verify that only authorized workloads are executed; and

(5) developing plans, budgets, and cost estimates and recommended courses of action for constructing or retrofitting such facilities.

(c) BRIEFING AND REPORT.—

(1) BRIEFING.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall provide to the congressional defense committees a briefing on progress made under the program required by subsection (a), including key findings

from prototype activities, threats, vulnerabilities, capability gaps, and resourcing requirements.

(2) REPORT.—Not later than one year after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees a report on the results of the program required by subsection (a), including—

(A) prototype results, technologies, or operational measures needed to improve the security of artificial intelligence data centers; and

(B) recommendations for further investments to address threats from nation-state adversaries.