AMENDMENT TO
RULES COMMITTEE PRINT 119–8
OFFERED BY MR. KRISHNAMOORTHI OF ILLINOIS

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

SEC. 15___. ANALYZING THREATS ASSOCIATED WITH FOREIGN ADVERSARY INTERNET OF THINGS MODULES AND MICROELECTRONICS TO THE DEPARTMENT OF DEFENSE.

(a) ASSESSMENT.—

(1) IN GENERAL.—Not later than 180 days after the date of enactment of this Act, the Secretary of Defense shall submit to the appropriate congressional committees an assessment of the threat posed by covered foreign adversary internet of things modules and other covered foreign adversary microelectronics to Department of Defense operations and national security, including—

(A) the threat of malign cyber activities of the People's Republic of China by means of such modules and microelectronics; and

(B) threats associated with Department of Defense supply chain dependencies with respect to the People's Republic of China.

(2) FORM.—The assessment required under subsection (a) shall be submitted in unclassified form, but may contain a classified annex.

(b) STRATEGY.—

(1) RISK MITIGATION STRATEGY.—Not later than 180 days after the date on which the assessment required under subsection (a) is required to be submitted, the Secretary of Defense shall submit to the appropriate congressional committees a strategy to—

(A) mitigate the risk of covered foreign adversary internet of things modules to the Department of Defense; and

(B) address risks to the Department of Defense associated with such other covered foreign adversary microelectronics as the Secretary of Defense deems appropriate.

(2) FORM.—The strategy required under subsection (a) shall be submitted in unclassified form, but may contain a classified annex.

(c) IMPLEMENTATION.—The Secretary of Defense, on not later than the date that is one year after the date

on which the strategy required under subsection (b) is submitted, shall update the appropriate congressional committees in written form regarding efforts to implement such strategy.

(d) DEFINITIONS.—In this section:

(1) The term ''covered foreign adversary internet of things module'' means a hardware component that enables a system, device, or other object to communicate, exchange data, and potentially initiate actions across a network interface, including sensors, actuators, embedded processors, and communication hardware, that is produced or sold by any entity that produces or sells such modules that the Secretary of Defense determines is domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of a country specified in section 4872(d)(2) of title 10, United States Code, and presents, in the sole determination of the Secretary of Defense, a significant national security threat based on a meaningful review of technical and other evidence.

(2) The term ''covered foreign adversary microelectronics'' shall refer to any microelectronic product that is produced or sold by an entity that the Secretary of Defense determines is domiciled in, is

headquartered in, has its principal place of business in, or is organized under the laws of a country specified in section 4872(d)(2) of title 10, United States Code.

☒