

**AMENDMENT TO**  
**RULES COMMITTEE PRINT 118-36**  
**OFFERED BY MR. KRISHNAMOORTHY OF ILLINOIS**

At the end of subtitle A of title VIII, add the following:

1 **SEC. 8 \_\_\_\_ . MITIGATING THREATS ASSOCIATED WITH FOR-**  
2 **EIGN ADVERSARY INTERNET OF THINGS**  
3 **MODULES AND MICROELECTRONICS TO THE**  
4 **DEPARTMENT OF DEFENSE.**

5 (a) ASSESSMENT.—

6 (1) IN GENERAL.—Not than 180 days after the  
7 date of enactment of this section, the Secretary of  
8 Defense shall submit to the appropriate congressional  
9 committees an assessment of the threats  
10 posed by covered foreign adversary internet of things  
11 modules and other covered foreign adversary micro-  
12 electronics to the operations of the Department of  
13 Defense and national security, including—

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

1 (B) threats arising from dependencies of  
2 supply chains of the Department relating to the  
3 People's Republic of China.

4 (2) FORM.—The assessment required under  
5 paragraph (1) shall be submitted in unclassified  
6 form, but may contain a classified annex.

7 (b) STRATEGY.—

8 (1) RISK MITIGATION STRATEGY.—Not than  
9 180 days after the date on which the assessment re-  
10 quired under subsection (a) is required to be sub-  
11 mitted, the Secretary of Defense shall submit to the  
12 appropriate congressional committees a strategy to  
13 mitigate—

14 (A) the risks to the Department of Defense  
15 from covered foreign adversary internet of  
16 things modules; and

17 (B) the risks to the Department of De-  
18 fense associated with such other covered foreign  
19 adversary microelectronics as determined appro-  
20 priate by the Secretary.

21 (2) FORM.—The strategy required under para-  
22 graph (1) shall be submitted in unclassified form,  
23 but may contain a classified annex.

24 (c) IMPLEMENTATION UPDATE.—Not later than one  
25 year after the date on which the strategy required under

1 subsection (b) is submitted, the Secretary of Defense shall  
2 submit to the appropriate congressional committees in  
3 writing an explanation of the actions taken to implement  
4 such strategy, including any actions to eliminate the use  
5 of covered foreign adversary internet of things modules in  
6 sensitive systems and devices of the Department of De-  
7 fense.

8 (d) DEFINITIONS.—In this section:

9 (1) The term “covered foreign adversary inter-  
10 net of things module” means a hardware component  
11 that enables a system, device, or other object to  
12 communicate, exchange data, and initiate actions  
13 across a network interface, including sensors, actu-  
14 ators, embedded processors, and communication  
15 hardware, that is produced or sold by an entity that  
16 produces or sells such modules that the Secretary of  
17 Defense determines is domiciled in, is headquartered  
18 in, has its principal place of business in, or is orga-  
19 nized under the laws of a country specified in section  
20 4872(d)(2) of title 10, United States Code, (includ-  
21 ing Quectel Wireless Solutions Co. Ltd. and  
22 Fibocom Wireless, Inc., and any successors, affili-  
23 ates, or subsidiaries of either such entity, to the ex-  
24 tent that such entities meet such criteria). and pre-  
25 sents, in the sole determination of the Secretary of

1 Defense, a significant national security threat based  
2 on a review of technical and other evidence.

3 (2) The term “covered foreign adversary micro-  
4 electronic” means a microelectronic product that is  
5 produced or sold by an entity that the Secretary of  
6 Defense determines is domiciled in, is headquartered  
7 in, has its principal place of business in, or is orga-  
8 nized under the laws of a country specified in section  
9 4872(d)(2) of title 10, United States Code.

