

**AMENDMENT TO RULES COMM. PRINT 117-13**  
**OFFERED BY MR. SCHWEIKERT OF ARIZONA**

Add at the end of subtitle D of title XV of division  
A the following:

1 **SEC. 15 \_\_\_\_ . IMPLEMENTATION OF CERTAIN CYBERSECU-**  
2 **RITY RECOMMENDATIONS; CYBER HYGIENE**  
3 **AND CYBERSECURITY MATURITY MODEL**  
4 **CERTIFICATION FRAMEWORK.**

5 (a) REPORT ON IMPLEMENTATION OF CERTAIN CY-  
6 BERSECURITY RECOMMENDATIONS.—Not later than 180  
7 days after the date of the enactment of this Act, the Sec-  
8 retary of Defense shall submit to the congressional defense  
9 committees a report regarding the plans of the Secretary  
10 to implement certain cybersecurity recommendations to  
11 ensure—

12 (1) the Chief Information Officer of the Depart-  
13 ment of Defense takes appropriate steps to ensure  
14 implementation of DC3I tasks;

15 (2) Department components develop plans with  
16 scheduled completion dates to implement any re-  
17 maining CDIP tasks overseen by the Chief Informa-  
18 tion Officer;

1           (3) the Deputy Secretary of Defense identifies  
2           a Department component to oversee the implementa-  
3           tion of any CDIP tasks not overseen by the Chief  
4           Information Officer and reports on progress relating  
5           to such implementation;

6           (4) Department components accurately monitor  
7           and report information on the extent that users have  
8           completed Cyber Awareness Challenge training, as  
9           well as the number of users whose access to the De-  
10          partment network was revoked because such users  
11          have not completed such training;

12          (5) the Chief Information Officer ensures all  
13          Department components, including DARPA, require  
14          their users to take Cyber Awareness Challenge train-  
15          ing;

16          (6) a Department component is directed to  
17          monitor the extent to which practices are imple-  
18          mented to protect the Department's network from  
19          key cyberattack techniques; and

20          (7) the Chief Information Officer assesses the  
21          extent to which senior leaders of the Department  
22          have more complete information to make risk-based  
23          decisions, and revise the recurring reports (or de-  
24          velop a new report) accordingly, including informa-

1           tion relating to the Department’s progress on imple-  
2           menting—

3                   (A) cybersecurity practices identified in  
4                   cyber hygiene initiatives; and

5                   (B) cyber hygiene practices to protect De-  
6                   partment networks from key cyberattack tech-  
7                   niques.

8           (b) REPORT ON CYBER HYGIENE AND CYBERSECU-  
9           RITY MATURITY MODEL CERTIFICATION FRAMEWORK.—

10                   (1) IN GENERAL.—Not later than 180 days  
11                   after the date of the enactment of this Act, the Sec-  
12                   retary of Defense shall submit to the congressional  
13                   defense committees and the Comptroller General of  
14                   the United States a report on the cyber hygiene  
15                   practices of the Department of Defense and the ex-  
16                   tent to which such practices are effective at pro-  
17                   tecting Department missions, information, system  
18                   and networks. The report shall include the following:

19                           (A) An assessment of each Department  
20                           component’s compliance with the requirements  
21                           and levels identified in the Cybersecurity Matu-  
22                           rity Model Certification framework.

23                           (B) For each Department component that  
24                           does not achieve the requirements for “good  
25                           cyber hygiene” as defined in CMMC Model

1           Version 1.02, a plan for how that component  
2           will implement security measures to bring it  
3           into compliance with good cyber hygiene re-  
4           quirements within one year, and a strategy for  
5           mitigating potential vulnerabilities and con-  
6           sequences until such requirements are imple-  
7           mented.

8           (2) COMPTROLLER GENERAL REVIEW.—Not  
9           later than 180 days after the submission of the re-  
10          port required under paragraph (1)), the Comptroller  
11          General of the United States shall conduct an inde-  
12          pendent review of the report and provide a briefing  
13          to the congressional defense committees on the find-  
14          ings of the review.

