

**AMENDMENT TO THE AMENDMENT IN THE  
NATURE OF A SUBSTITUTE TO H.R. 3935  
OFFERED BY MR. ROUZER OF NORTH CAROLINA**

At the end of title VIII, add the following:

1 **SECTION \_\_\_\_ . SECURING AIRCRAFT AVIONIC SYSTEMS.**

2 Section 506(a) of the FAA Reauthorization Act of  
3 2018 (49 U.S.C. 44704 note) is amended—

4 (1) in the matter preceding paragraph (1)—

5 (A) by striking “consider” and inserting  
6 “revise”; and

7 (B) by striking “revising” and inserting  
8 “existing”;

9 (2) in paragraph (1) by striking “and” at the  
10 end;

11 (3) in paragraph (2) by striking the period at  
12 the end and inserting “; and”; and

13 (4) by adding at the end the following:

14 “(3) to require that aircraft avionics serial net-  
15 works used for flight guidance or aircraft control be  
16 monitored to verify they have not been compromised  
17 by unauthorized external and internal access.”.

1 **SEC. \_\_\_\_ . COMPTROLLER REVIEW AND REPORT OF CYBER-**  
2 **SECURITY OF COMMERCIAL AVIATION AVI-**  
3 **ONICS.**

4 (a) IN GENERAL.—The Comptroller General of the  
5 United States shall conduct a review on the consideration,  
6 identification, and inclusion of aircraft cybersecurity into  
7 the strategic framework for aviation security and further  
8 as part of the Federal Aviation Administration’s cyberse-  
9 curity strategy.

10 (b) CONTENTS OF REVIEW.—The review under sub-  
11 section (a) shall assess—

12 (1) how onboard aircraft cybersecurity risks  
13 and vulnerabilities are defined and accounted for in  
14 the strategy aviation security framework, particu-  
15 larly in pillar 2 “protect and defend FAA networks  
16 and systems to mitigate risks to FAA missions and  
17 service delivery”;

18 (2) how onboard aircraft cybersecurity, particu-  
19 larly of the aircraft avionics, is considered, incor-  
20 porated, and prioritized in the cybersecurity strategy  
21 pursuant to section 509 of the FAA Reauthorization  
22 Act of 2018 (49 U.S.C. 44903 note);

23 (3) how roles and responsibilities for aircraft  
24 and ground systems cybersecurity are differentiated  
25 and enforced between the Transportation Security  
26 Agency and Federal Aviation Administration;

1           (4) how aircraft and ground systems cybersecu-  
2           rity vulnerabilities are being identified and  
3           prioritized for mitigation, particularly considering  
4           the commercial technology ecosystem; and

5           (5) the budgets of the responsible parties, as  
6           identified in subsection (b)(1), to satisfy those miti-  
7           gation requirements necessary to secure the aviation  
8           ecosystem from onboard cybersecurity vulnerabilities.

