

114TH CONGRESS
2D SESSION

S. _____

To require the disclosure of information relating to cyberattacks on aircraft systems and maintenance and ground support systems for aircraft, to identify and address cybersecurity vulnerabilities to the United States commercial aviation system, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. MARKEY introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To require the disclosure of information relating to cyberattacks on aircraft systems and maintenance and ground support systems for aircraft, to identify and address cybersecurity vulnerabilities to the United States commercial aviation system, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cybersecurity Stand-
5 ards for Aircraft to Improve Resilience Act of 2016” or
6 the “Cyber AIR Act”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) COVERED AIR CARRIER.—The term “cov-
4 ered air carrier” means an air carrier or a foreign
5 air carrier (as those terms are defined in section
6 40102 of title 49, United States Code).

7 (2) COVERED MANUFACTURER.—The term
8 “covered manufacturer” means an entity that—

9 (A) manufactures or otherwise produces
10 aircraft and holds a production certificate under
11 section 44704(c) of title 49, United States
12 Code; or

13 (B) manufactures or otherwise produces
14 electronic control, communications, mainte-
15 nance, or ground support systems for aircraft.

16 (3) CYBERATTACK.—The term “cyberattack”
17 means the unauthorized access to aircraft electronic
18 control or communications systems or maintenance
19 or ground support systems for aircraft, either wire-
20 lessly or through a wired connection.

21 (4) CRITICAL SOFTWARE SYSTEMS.—The term
22 “critical software systems” means software systems
23 that can affect control over the operation of an air-
24 craft.

25 (5) ENTRY POINT.—The term “entry point”
26 means the means by which signals to control a sys-

1 **SEC. 4. INCORPORATION OF CYBERSECURITY INTO RE-**
2 **QUIREMENTS FOR AIR CARRIER OPERATING**
3 **CERTIFICATES AND PRODUCTION CERTIFI-**
4 **CATES.**

5 (a) REGULATIONS.—Not later than 270 days after
6 the date of the enactment of this Act, the Secretary of
7 Transportation, in consultation with the Secretary of De-
8 fense, the Secretary of Homeland Security, the Attorney
9 General, the Federal Communications Commission, and
10 the Director of National Intelligence, shall prescribe regu-
11 lations to incorporate requirements relating to cybersecu-
12 rity into the requirements for obtaining an air carrier op-
13 erating certificate or a production certificate under chap-
14 ter 447 of title 49, United States Code.

15 (b) REQUIREMENTS.—In prescribing the regulations
16 required by subsection (a), the Secretary shall—

17 (1) require all entry points to the electronic sys-
18 tems of each aircraft operating in United States air-
19 space and maintenance or ground support systems
20 for such aircraft to be equipped with reasonable
21 measures to protect against cyberattacks, including
22 the use of isolation measures to separate critical
23 software systems from noncritical software systems;

24 (2) require the periodic evaluation of the meas-
25 ures described in paragraph (1) for security
26 vulnerabilities using best security practices, includ-

1 ing the appropriate application of techniques such as
2 penetration testing, in consultation with the Sec-
3 retary of Defense, the Secretary of Homeland Secu-
4 rity, the Attorney General, the Federal Communica-
5 tions Commission, and the Director of National In-
6 telligence; and

7 (3) require the measures described in para-
8 graph (1) to be periodically updated based on the re-
9 sults of the evaluations conducted under paragraph
10 (2).

11 **SEC. 5. ANNUAL REPORT ON CYBERATTACKS ON AIRCRAFT**
12 **SYSTEMS AND MAINTENANCE AND GROUND**
13 **SUPPORT SYSTEMS.**

14 (a) IN GENERAL.—Not later than one year after the
15 date of the enactment of this Act, and annually thereafter,
16 the Administrator of the Federal Aviation Administration
17 shall submit to the appropriate committees of Congress
18 a report on attempted and successful cyberattacks on any
19 system on board an aircraft, whether or not the system
20 is critical to the safe and secure operation of the aircraft,
21 and on maintenance or ground support systems for air-
22 craft, that includes—

23 (1) the number of such cyberattacks during the
24 year preceding the submission of the report;

25 (2) with respect to each such cyberattack—

1 (A) an identification of the system that
2 was targeted;

3 (B) a description of the effect on the safe-
4 ty of the aircraft as a result of the cyberattack;
5 and

6 (C) a description of the measures taken to
7 counter or mitigate the cyberattack;

8 (3) recommendations for preventing a future
9 cyberattack;

10 (4) an analysis of potential vulnerabilities to
11 cyberattacks in systems on board an aircraft and in
12 maintenance or ground support systems for aircraft;
13 and

14 (5) recommendations for improving the regu-
15 latory oversight of aircraft cybersecurity.

16 (b) FORM OF REPORT.—The report required by sub-
17 section (a) shall be submitted in unclassified form, but
18 may include a classified annex.

19 **SEC. 6. MANAGING CYBERSECURITY RISKS OF CONSUMER**
20 **COMMUNICATIONS EQUIPMENT.**

21 (a) IN GENERAL.—The Commercial Aviation Com-
22 munications Safety and Security Leadership Group estab-
23 lished by the memorandum of understanding between the
24 Department of Transportation and the Federal Commu-
25 nications Commission entitled “Framework for DOT-FCC

1 Coordination of Commercial Aviation Communications
2 Safety and Security Issues” and dated January 29, 2016
3 (in this section known as the “Leadership Group”) shall
4 be responsible for evaluating the cybersecurity
5 vulnerabilities of broadband wireless communications
6 equipment designed for consumer use on board aircraft
7 operated by covered air carriers that is installed before,
8 on, or after, or is proposed to be installed on or after,
9 the date of the enactment of this Act.

10 (b) RESPONSIBILITIES.—To address cybersecurity
11 risks arising from malicious use of communications tech-
12 nologies on board aircraft operated by covered air carriers,
13 the Leadership Group shall—

14 (1) ensure the development of effective methods
15 for preventing foreseeable cyberattacks that exploit
16 broadband wireless communications equipment de-
17 signed for consumer use on board such aircraft; and

18 (2) require the implementation by covered air
19 carriers, covered manufacturers, and communica-
20 tions service providers of all technical and oper-
21 ational security measures that are deemed necessary
22 and sufficient by the Leadership Group to prevent
23 cyberattacks described in paragraph (1).

24 (c) REPORT REQUIRED.—

1 (1) IN GENERAL.—Not later than one year
2 after the date of the enactment of this Act, and an-
3 nually thereafter, the Leadership Group shall submit
4 to the Committee on Commerce, Science, and Trans-
5 portation of the Senate and the Committee on
6 Transportation and Infrastructure of the House of
7 Representatives a report on—

8 (A) the technical and operational security
9 measures developed to prevent foreseeable
10 cyberattacks that exploit broadband wireless
11 communications equipment designed for con-
12 sumer use on board aircraft operated by cov-
13 ered air carriers; and

14 (B) the steps taken by covered air carriers,
15 covered manufacturers, and communications
16 service providers to implement the measures de-
17 scribed in subparagraph (A).

18 (2) FORM OF REPORT.—The report required by
19 paragraph (1) shall be submitted in unclassified
20 form, but may include a classified annex.