

116TH CONGRESS  
1ST SESSION

# S. 2181

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

JULY 18, 2019

Mr. MARKEY (for himself and Mr. BLUMENTHAL) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

## 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 2019” 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 on, or after, or is proposed to be installed on or after,  
2 the date of the enactment of this Act.

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

7 (1) ensure the development of effective methods  
8 for preventing foreseeable cyberattacks that exploit  
9 broadband wireless communications equipment de-  
10 signed for consumer use on board such aircraft; and

11 (2) require the implementation by covered air  
12 carriers, covered manufacturers, and communica-  
13 tions service providers of all technical and oper-  
14 ational security measures that are deemed necessary  
15 and sufficient by the Leadership Group to prevent  
16 cyberattacks described in paragraph (1).

17 (c) REPORT REQUIRED.—Not later than one year  
18 after the date of the enactment of this Act, and annually  
19 thereafter, the Leadership Group shall submit to the Com-  
20 mittee on Commerce, Science, and Transportation of the  
21 Senate and the Committee on Transportation and Infra-  
22 structure of the House of Representatives a report on—

23 (1) the technical and operational security meas-  
24 ures developed to prevent foreseeable cyberattacks  
25 that exploit broadband wireless communications

1 equipment designed for consumer use on board air-  
2 craft operated by covered air carriers; and

3 (2) the steps taken by covered air carriers, cov-  
4 ered manufacturers, and communications service  
5 providers to implement the measures described in  
6 paragraph (1).

○