II

114TH CONGRESS
2D SESSION

S. 2764

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

APRIL 7, 2016

Mr. MARKEY 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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity Standards for Aircraft to Improve Resilience Act of 2016'' or the ''Cyber AIR Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) COVERED AIR CARRIER.—The term ''covered air carrier'' means an air carrier or a foreign air carrier (as those terms are defined in section 40102 of title 49, United States Code).

(2) COVERED MANUFACTURER.—The term ''covered manufacturer'' means an entity that—

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

(B) manufactures or otherwise produces electronic control, communications, maintenance, or ground support systems for aircraft.

(3) CYBERATTACK.—The term ''cyberattack'' means the unauthorized access to aircraft electronic control or communications systems or maintenance or ground support systems for aircraft, either wirelessly or through a wired connection.

(4) CRITICAL SOFTWARE SYSTEMS.—The term ''critical software systems'' means software systems that can affect control over the operation of an aircraft.

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

tem on board an aircraft or a maintenance or ground support system for aircraft may be sent or received.

SEC. 3. DISCLOSURE OF CYBERATTACKS BY THE AVIATION INDUSTRY.

(a) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Transportation shall prescribe regulations requiring covered air carriers and covered manufacturers to disclose to the Federal Aviation Administration any attempted or successful cyberattack on any system on board an aircraft, whether or not the system is critical to the safe and secure operation of the aircraft, or any maintenance or ground support system for aircraft, operated by the air carrier or produced by the manufacturer, as the case may be.

(b) USE OF DISCLOSURES BY THE FEDERAL AVIATION ADMINISTRATION.—The Administrator of the Federal Aviation Administration shall use the information obtained through disclosures made under subsection (a) to improve the regulations required by section 4 and to notify air carriers, aircraft manufacturers, and other Federal agencies of cybersecurity vulnerabilities in systems on board an aircraft or maintenance or ground support systems for aircraft.

SEC. 4. INCORPORATION OF CYBERSECURITY INTO REQUIREMENTS FOR AIR CARRIER OPERATING CERTIFICATES AND PRODUCTION CERTIFICATES.

(a) REGULATIONS.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Transportation, in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Attorney General, the Federal Communications Commission, and the Director of National Intelligence, shall prescribe regulations to incorporate requirements relating to cybersecurity into the requirements for obtaining an air carrier operating certificate or a production certificate under chapter 447 of title 49, United States Code.

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

(1) require all entry points to the electronic systems of each aircraft operating in United States airspace and maintenance or ground support systems for such aircraft to be equipped with reasonable measures to protect against cyberattacks, including the use of isolation measures to separate critical software systems from noncritical software systems;

(2) require the periodic evaluation of the measures described in paragraph (1) for security vulnerabilities using best security practices, includ-

ing the appropriate application of techniques such as penetration testing, in consultation with the Secretary of Defense, the Secretary of Homeland Security, the Attorney General, the Federal Communications Commission, and the Director of National Intelligence; and

(3) require the measures described in paragraph (1) to be periodically updated based on the results of the evaluations conducted under paragraph (2).

SEC. 5. ANNUAL REPORT ON CYBERATTACKS ON AIRCRAFT SYSTEMS AND MAINTENANCE AND GROUND SUPPORT SYSTEMS.

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

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

(2) with respect to each such cyberattack—

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

(B) a description of the effect on the safety of the aircraft as a result of the cyberattack; and

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

(3) recommendations for preventing a future cyberattack;

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

(5) recommendations for improving the regulatory oversight of aircraft cybersecurity.

(b) FORM OF REPORT.—The report required by subsection (a) shall be submitted in unclassified form, but may include a classified annex.

SEC. 6. MANAGING CYBERSECURITY RISKS OF CONSUMER COMMUNICATIONS EQUIPMENT.

(a) IN GENERAL.—The Commercial Aviation Communications Safety and Security Leadership Group established by the memorandum of understanding between the Department of Transportation and the Federal Communications Commission entitled ''Framework for DOT–

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

(b) RESPONSIBILITIES.—To address cybersecurity risks arising from malicious use of communications technologies on board aircraft operated by covered air carriers, the Leadership Group shall—

(1) ensure the development of effective methods for preventing foreseeable cyberattacks that exploit broadband wireless communications equipment designed for consumer use on board such aircraft; and

(2) require the implementation by covered air carriers, covered manufacturers, and communications service providers of all technical and operational security measures that are deemed necessary and sufficient by the Leadership Group to prevent cyberattacks described in paragraph (1).

(c) REPORT REQUIRED.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, and annually thereafter, the Leadership Group shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives a report on—

(A) the technical and operational security measures developed to prevent foreseeable cyberattacks that exploit broadband wireless communications equipment designed for consumer use on board aircraft operated by covered air carriers; and

(B) the steps taken by covered air carriers, covered manufacturers, and communications service providers to implement the measures described in subparagraph (A).

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

○