AMENDMENT NO. _______ Calendar No. _______

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

IN THE SENATE OF THE UNITED STATES—114th Cong., 2d Sess.

S. 2658

To amend title 49, United States Code, to authorize appropriations for the Federal Aviation Administration for fiscal years 2016 through 2017, and for other purposes.

Referred to the Committee on _______ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENTS intended to be proposed by Mr. MARKEY

Viz:
1. On page 275, between lines 22 and 23, insert the following:
   (a) DEFINITIONS.—In this section:
   (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(e) 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 system on board an aircraft or a maintenance or ground support system for aircraft may be sent or received.

On page 275, line 23, strike "(a) IN GENERAL.—" and insert "(b) ACTIONS OF THE ADMINISTRATOR.—".
On page 276, strike lines 7 through 10.

On page 276, strikes lines 14 through 18, and insert the following:

(c) Disclosure of Cyberattacks by the Aviation Industry.—

(1) 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.

(2) 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 subsection (d) and to notify air carriers, aircraft manufacturers, and other Federal agencies of cybersecurity vulnerabilities in systems on board an air-
craft or maintenance or ground support systems for
aircraft.

(d) INCORPORATION OF CYBERSECURITY INTO RE-
quirements for Air Carrier Operating Certifi-
cates and Production Certificates.—

(1) Regulations.—Not later than 270 days
after the date of the enactment of this Act, the Sec-
retary of Transportation, in consultation with the
Secretary of Defense, the Secretary of Homeland Se-
curity, the Attorney General, the Federal Commu-
ications Commission, and the Director of National
Intelligence, shall prescribe regulations to incor-
porate requirements relating to cybersecurity into
the requirements for obtaining an air carrier oper-
ating certificate or a production certificate under
chapter 447 of title 49, United States Code.

(2) REQUIREMENTS.—In prescribing the regu-
lations required by paragraph (1), the Secretary
shall—

(A) require all entry points to the elec-
tronic 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 isola-
tion measures to separate critical software sys-

tems from noncritical software systems;

(B) require the periodic evaluation of the

measures described in subparagraph (A) for se-

curity vulnerabilities using best security prac-

tices, including the appropriate application of

techniques such as penetration testing, in con-

sultation with the Secretary of Defense, the

Secretary of Homeland Security, the Attorney

General, the Federal Communications Commis-

sion, and the Director of National Intelligence;

and

(C) require the measures described in sub-

paragraph (A) to be periodically updated based

on the results of the evaluations conducted

under subparagraph (B).

(c) ANNUAL REPORT ON CYBERATTACKS ON AIR-

CRAFT SYSTEMS AND MAINTENANCE AND GROUND SUP-

PORT SYSTEMS.—

(1) IN GENERAL.—Not later than one year

after the date of the enactment of this Act, the Ad-

ministrator of the Federal Aviation Administration

shall submit to the appropriate committees of Con-

gress a report on—
(A) 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—

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

(ii) with respect to each such cyberattack—

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

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

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

(iii) recommendations for preventing a future cyberattack;

(iv) an analysis of potential vulnerabilities to cyberattacks in systems on board an aircraft and in maintenance or ground support systems for aircraft; and
(v) recommendations for improving
the regulatory oversight of aircraft cyber-
security; and

(B) the progress made toward imple-
menting the requirements under subsection (b).

(2) FORM OF REPORT; PUBLIC AVAILABILITY.—

(A) FORM OF REPORT.—Each report re-
quired by paragraph (1) shall be submitted in
unclassified form, but may include a classified
annex.

(B) PUBLIC AVAILABILITY.—The Adminis-
trator shall make the unclassified portion of the
report required by paragraph (1) available to
the public, with any confidential business infor-

(f) MANAGING CYBERSECURITY RISKS OF CON-
SUMER COMMUNICATIONS EQUIPMENT.—

(1) IN GENERAL.—The Commercial Aviation
Communications Safety and Security Leadership
Group established by the memorandum of under-
standing between the Department of Transportation
and the Federal Communications Commission enti-
tled “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 air-
craft operated by covered air carriers that is in-
stalled before, on, or after, or is proposed to be in-
stalled on or after, the date of the enactment of this
Act.

(2) RESPONSIBILITIES.—To address cybersecurity
risks arising from malicious use of communica-
tions technologies on board aircraft operated by cov-
ered air carriers, the Leadership Group shall—

(A) 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

(B) require the implementation by covered
air carriers, covered manufacturers, and com-
munications service providers of all technical
and operational security measures that are
deemed necessary and sufficient by the Leader-
ship Group to prevent cyberattacks described in
subparagraph (A).

(3) REPORT REQUIRED.—
(A) 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—

(i) 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

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

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

(4) PUBLIC AVAILABILITY.—The Leadership Group shall make the unclassified portion of the re-
port required by subparagraph (A) available to the public, with any confidential business information redacted.