S 679

Cyber AIR Act

Congress: 115 (2017–2019, Ended)
Chamber: Senate
Policy Area: Transportation and Public Works
Introduced: Mar 21, 2017
Current Status: Read twice and referred to the Committee on Commerce, Science, and Transportation.
Latest Action: Read twice and referred to the Committee on Commerce, Science, and Transportation. (Mar 21, 2017)
Official Text: https://www.congress.gov/bill/115th-congress/senate-bill/679

Sponsor

Name: Sen. Markey, Edward J. [D-MA]
Party: Democratic • **State:** MA • **Chamber:** Senate

Cosponsors (1 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Blumenthal, Richard [D-CT]	D · CT		Mar 21, 2017

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Referred To	Mar 21, 2017

Subjects & Policy Tags

Policy Area:

Transportation and Public Works

Related Bills

No related bills are listed.

Summary (as of Mar 21, 2017)

Cybersecurity Standards for Aircraft to Improve Resilience Act of 2017 or the Cyber AIR Act

This bill directs the Department of Transportation (DOT) to require domestic or foreign air carriers and manufacturers of aircraft or electronic control, communications, maintenance, or ground support systems for aircraft to disclose to the Federal Aviation Administration (FAA) any attempted or successful cyberattack against any system on board an aircraft or against any maintenance or ground support system for aircraft.

The FAA shall use the information obtained through such disclosures to: (1) improve the regulations (to be prescribed by DOT) to incorporate requirements relating to cybersecurity into the requirements for obtaining an air carrier operating certificate or a production certificate; and (2) 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.

In prescribing such regulations, DOT must require: (1) all entry points to the electronic systems of each aircraft operating in U.S. airspace and maintenance or ground support systems for such aircraft to be equipped with reasonable measures to protect against cyberattacks; and (2) the periodic evaluation of, and updates to, such measures for security vulnerabilities using best security practices.

The Commercial Aviation Communications Safety and Security Leadership Group shall: (1) be responsible for evaluating the cybersecurity vulnerabilities of certain broadband wireless communications equipment designed for consumer use on board aircraft; and (2) require the implementation by air carriers, manufacturers, and communications service providers of technical and operational security measures it deems necessary to prevent cyberattacks that exploit such equipment.

Actions Timeline

- **Mar 21, 2017:** Introduced in Senate
- **Mar 21, 2017:** Read twice and referred to the Committee on Commerce, Science, and Transportation.