AMENDMENT TO
RULES COMMITTEE PRINT 118–10
OFFERED BY MR. GALLAGHER OF WISCONSIN

At the end of title XVIII, add the following:

SEC. ___ . AIR CARRIER CYBERSECURITY.

(a) Risk Assessments for Air Carriers.—

(1) In General.—All covered air carriers shall, not later than September 30, 2024, and annually thereafter, conduct a self-assessment and third-party assessment of the risk of such air carrier to a major cyber attacks on the onboard networked systems of an aircraft operated by the air carrier that could significantly disrupt the flight operations of such carrier for more than 48 hours.

(2) Contents.—The assessments described in paragraph (1) shall include an identification and analysis of—

(A) potential cyber attack scenarios, particularly scenarios involving a covered nation;

(B) single points of failure for the covered air carriers;

(C) defense and mitigation measures of the air carrier in the case of a cyber attack; and
(D) the risks to and from critical vendors
and service providers.

(3) Provision of Assessment.—Each air carrier conducting an assessment required under paragraph (1) shall provide such assessment to the Administrators, who shall provide such assessment to the Secretary of Transportation, the Secretary of Defense, and the Secretary of Homeland Security.

(b) Resilience Plan.—All covered air carriers shall, not later than December 31, 2024, and annually thereafter, submit a cyber resilience plan to the Administrators. Such resilience plan shall include—

(1) plans for operations continuity in the event of a cyber attack on the air carrier; and

(2) plans for the recovery and restoration of flight operations in stages following a major stoppage caused by a cyber attack on the air carrier or the critical vendors and suppliers of such air carrier.

(c) Regulations.—Not later than 120 days after the date of enactment of this Act, the Administrators, acting in coordination, shall issue regulations implementing this section. Such regulations shall—

(1) provide further detail regarding—
(A) what information shall be included in
the assessments and resilience plans described
in this section; and

(B) the format such information shall be
provided in; and

(2) provide a mechanism for the assessments
and resilience plans to be submitted in a manner to
protect trade secrets, business confidentiality, and
proprietary information and

(3) ensure that such regulations do not conflict
with existing regulations promulgated by the Trans-
portation Security Administration and Federal Avia-
tion Administration.

(d) REPORTING.—After September 30, 2024, but be-
fore September 30, 2025, and annually thereafter—

(1) the Administrators shall submit to the ap-
propriate congressional committees a report summa-
rizing the results of the assessments carried out
under this section and the overall state of the cyber-
security of covered air carriers; and

(2) the Secretary of Defense shall submit to the
appropriate congressional committees a report de-
scribing the risks to military readiness of the United
States deriving from the risk of cyber attacks on
covered air carriers.
(e) DEFINITIONS.—In this section:

(1) ADMINISTRATORS.—The term “Administrators” means the Administrator of the Transportation Security Administration and the Administrator of the Federal Aviation Administration.

(2) AIR CARRIER; AIRCRAFT.—The terms “air carrier” and “aircraft” have the meanings given such terms in section 40102(a) of title 49, United States Code.

(3) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term “appropriate congressional committees” means—

(A) the Committee on Armed Services, the Committee on Homeland Security and Government Affairs, and the Committee on Commerce, Science, and Transportation of the Senate; and

(B) the Committee on Armed Services, the Committee on Oversight and Reform, and the Committee on Transportation and Infrastructure of the House of Representatives.

(4) COVERED AIR CARRIERS.—The term “covered air carrier” means any air carrier that owns at least 700 commercial aircraft.
(5) COVERED NATION.—The term “covered nation” has the meaning given such term in section 4872(d) of title 10, United States Code.

(6) ONBOARD NETWORKED SYSTEMS.—The term “onboard networked systems” means, with respect to an aircraft—

(A) avionics, communications, and flight control systems;

(B) information and management systems;

(C) passenger information and entertainment systems; and

(D) any other connected software system on board an aircraft.

(7) THIRD-PARTY ASSESSMENT.—The term “third-party assessment” means an assessment of the risks posed by vendors, suppliers, and service providers for air carriers and other third-party relationships across an air carrier’s supply chain.