I

117TH CONGRESS
2D SESSION

H. R. 9709

To direct the Administrator of the Federal Aviation Administration to issue regulations, policy, and guidance to ensure the safety of the aviation system, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JANUARY 3, 2023

Mr. GRAVES of Louisiana introduced the following bill; which was referred to the Committee on Transportation and Infrastructure

---

A BILL

To direct the Administrator of the Federal Aviation Administration to issue regulations, policy, and guidance to ensure the safety of the 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 ''Protecting the Safety of Air Traffic Control and the Aviation System Act''.

SEC. 2. FINDINGS.

Congress finds the following:

(1) Since its establishment in 1958, the Federal Aviation Administration, originally named the Federal Aviation Agency, has been responsible for—

(A) promoting the safe flight of civil aircraft in air commerce;

(B) ensuring the safe, secure, and efficient use of the national airspace system and provision of air navigation services; and

(C) overseeing the certification and continued airworthiness of aircraft and other aeronautical products.

(2) Congress has repeatedly tasked the Federal Aviation Administration with responsibility for securing the national airspace system, including the air traffic control system, airspace management, civil aircraft, and aeronautical products and articles through safety regulation and oversight. These mandates have routinely included protecting against associated cyber threats affecting aviation safety or the Administration's provision of safe, secure, and efficient air navigation services and airspace management.

(3) In 2003, Congress passed the Vision 100—Century of Aviation Reauthorization Act, which directed the Federal Aviation Administration to de-

velop and submit a report on an integrated plan to ensure that the Next Generation Air Transportation System meets future air transportation safety, security, mobility, efficiency, and capacity needs.

(4) In 2012, Congress passed the FAA Modernization and Reform Act of 2012, which directed the Federal Aviation Administration to develop a NextGen Implementation Plan with a detailed description of how the agency is implementing the Next Generation Air Transportation System, and contingency plans for dealing with the degradation of the System in the event of a natural disaster, major equipment failure, or act of terrorism.

(5) In 2016, Congress passed the FAA Extension, Safety, and Security Act of 2016, which established requirements for the Federal Aviation Administration to enhance the national airspace system's cybersecurity and included mandates for the Administration to—

(A) develop a cybersecurity strategic plan;

(B) coordinate with other Federal agencies to identify cyber vulnerabilities;

(C) develop a cyber threat model; and

(D) complete a comprehensive, strategic policy framework to identify and mitigate cybersecurity risks to the air traffic control system.

(6) In 2018, Congress passed the FAA Reauthorization Act of 2018 which—

(A) authorized funding for the construction of Federal Aviation Administration facilities dedicated to improving the cybersecurity of the national airspace system;

(B) required the Federal Aviation Administration to publish a 5-year roadmap for the introduction of civil unmanned aircraft systems into the national airspace system with an update on the advancement of technologies needed to integrate unmanned aircraft systems into the national airspace system, including decision making by adaptive systems and cyber physical systems security;

(C) required the Federal Aviation Administration to develop a plan to allow for the implementation of unmanned aircraft systems traffic management services, including an assessment of cybersecurity protections, data integrity, and national and homeland security benefits of such a system;

(D) mandated that the Federal Aviation Administration consider revising Federal Aviation Administration regulations regarding airworthiness certification to address cybersecurity for avionics systems, including software components and to require that aircraft avionics systems used for flight guidance or aircraft control be secured against unauthorized access and that avionics systems be protected from unauthorized external and internal access;

(E) required the Federal Aviation Administration to review and update its comprehensive, strategic policy framework for cybersecurity to assess the degree to which the framework identifies and addresses known cybersecurity risks associated with the aviation system, and evaluate existing short- and long-term objectives for addressing cybersecurity risks to the national airspace system;

(F) created a Chief Technology Officer position within the Federal Aviation Administration to be responsible for, among other things, coordinating the implementation, operation, maintenance, and cybersecurity of technology programs relating to the air traffic control sys-

tem with the aviation industry and other Federal agencies;

(G) directed the National Academy of Sciences to study the cybersecurity workforce of the Federal Aviation Administration in order to develop recommendations to increase the size, quality, and diversity of such workforce; and

(H) required the Federal Aviation Administration to develop a comprehensive plan to attract, develop, train, and retain talented individuals in the fields of systems engineering, systems architecture, systems integration, digital communications, and cybersecurity.

(7) Congress has tasked the Federal Aviation Administration with being the primary Federal agency to assess and address the threats posed from cyber incidents relating to United States Government-provided air traffic control and air traffic management services and the threats posed from cyber incidents relating to civil aircraft, aeronautical products and articles, aviation networks, aviation systems, services, and operations, and the aviation industry.

(8) Since 2005, the Federal Aviation Administration has been addressing cyber vulnerabilities in

civil aircraft and aeronautical products and articles during the safety certification process.

(9) Congress has received and reviewed testimony, briefings, and documentation on the potential risks of cyber incidents relating to Federal Aviation Administration-provided air navigation services and airspace management, civil aircraft, aeronautical products and articles, aviation networks, aviation systems, services, and operations, and the aviation industry. This testimony and documentation demonstrate the complicated and increasingly interconnected relationship between aviation safety; the safe, secure, and efficient provision of air navigation services; and cybersecurity for both Federal Aviation Administration-provided air navigation services and airspace management, and civil aircraft, aeronautical products and articles, aviation networks, aviation systems, services, and operations.

(10) This testimony and documentation also demonstrate the need for the Federal Aviation Administration to issue specific regulations, policy, and guidance that are standardized and harmonized, where appropriate and consistent with the interests of safety in air commerce and national security with

key international partners and International Civil Aviation Organization.

SEC. 3. NATIONAL AIRSPACE SYSTEM, AIR TRAFFIC CONTROL, AND AIRSPACE MANAGEMENT SAFETY.

Section 106(f)(2) of title 49, United States Code, is amended—

(1) in subparagraph (A)(ii) by striking ''and maintenance'' and inserting ''maintenance, and security (including cybersecurity)''; and

(2) in subparagraph (D) by inserting ''or any other Federal agency'' after ''Department of Transportation''.

SEC. 4. AVIATION PRODUCT SAFETY.

(a) CYBERSECURITY STANDARDS.—Section 44701(a) of title 49, United States Code, is amended—

(1) in paragraph (1) by inserting ''cybersecurity,'' after ''quality of work,''; and

(2) in paragraph (5)—

(A) by inserting ''cybersecurity and'' after ''standards for''; and

(B) by striking ''procedure'' and inserting ''procedures''.

(b) EXCLUSIVE RULEMAKING AUTHORITY.—Section 44701 of title 49, United States Code, is amended by adding at the end the following:

''(g) EXCLUSIVE RULEMAKING AUTHORITY.—Notwithstanding any other provision of law and except as provided in section 40131, to the extent that a provision of law authorizes any Federal agency that is not the Department of Transportation, or component thereof, to issue regulations under such provision for purposes of assuring civil aircraft, aircraft engine, propeller, and appliance cybersecurity, the Administrator of the Federal Aviation Administration shall have the exclusive authority to prescribe regulations subject to such provision.''.

SEC. 5. AIRPORTS.

(a) IN GENERAL.—Section 44706(b) of title 49, United States Code, is amended—

(1) in paragraph (1) by striking ''and'' at the end;

(2) in paragraph (2) by striking the period at the end and inserting ''; and''; and

(3) by adding at the end the following:

''(3) such cybersecurity standards as the Administrator may prescribe.''.

(b) CLASSIFICATION.—Not later than 180 days after the date of enactment of this Act, the Secretary of Transportation shall revise section 15.5 of title 49, Code of Federal Regulations, to classify information about cybersecurity standards for airports holding an airport operating

certificate issued under section 44706 of title 49, United States Code, as sensitive security information.

SEC. 6. FEDERAL AVIATION ADMINISTRATION REGULATIONS, POLICY, AND GUIDANCE.

(a) IN GENERAL.—Chapter 401 of title 49, United States Code, is amended by adding at the end the following new section:

"§ 40131. National airspace system cyber threat management process

''(a) ESTABLISHMENT.—The Administrator of the Federal Aviation Administration shall establish a national airspace system cyber threat management process to protect the national airspace system cyber environment, including the safety, security, and efficiency of the airspace management services provided by the Administration.

''(b) ISSUES TO BE ADDRESSED.—In establishing the national airspace system cyber threat management process under subsection (a), the Administrator shall, at a minimum—

''(1) monitor the national airspace system cyber environment;

''(2) in consultation with appropriate Federal agencies, evaluate the cyber threat landscape for the national airspace system, including updating such

evaluation on both annual and threat-based timelines;

''(3) conduct national airspace system cyber incident analyses;

''(4) create a cyber common operating picture for the national airspace system cyber environment;

''(5) determine whether, and if so how, to conduct active cyber defense;

''(6) coordinate national airspace system cyber incident responses with other appropriate Federal agencies;

''(7) track cyber incident detection, response, mitigation implementation, recovery, and closure;

''(8) establish a process to collect relevant national airspace system cyber incident data from internal and external stakeholders; and

''(9) any other matter the Administrator determines appropriate.

''(c) DEFINITIONS.—In this section, the following definitions apply:

''(1) ACTIVE CYBER DEFENSE.—The term 'active cyber defense' means the use of cyber enforcement capabilities that actively interdict the movement or processing of data to mitigate a cyber threat.

''(2) CYBER COMMON OPERATING PICTURE.—The term 'cyber common operating picture' means the correlation of a detected cyber incident or cyber threat in the national airspace system and other operational anomalies to provide a holistic view of potential cause and impact.

''(3) CYBER ENVIRONMENT.—The term 'cyber environment' means the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers.

''(4) CYBER INCIDENT.—The term 'cyber incident' means an action that creates noticeable degradation, disruption, or destruction to the cyber environment of—

''(A) the national airspace system;

''(B) civil aircraft information, data, networks, systems, services, operations and technology; or

''(C) aeronautical products and articles.

''(5) CYBER THREAT.—The term 'cyber threat' means the threat of an action that, if carried out, would constitute a cyber incident, an intentional un-

authorized electronic interaction, or an electronic attack.

''(6) ELECTRONIC ATTACK.—The term 'electronic attack' means the use of electromagnetic spectrum energy to impede operations in the cyber environment, including through techniques such as jamming or spoofing.

''(7) INTENTIONAL UNAUTHORIZED ELECTRONIC INTERACTION.—The term 'intentional unauthorized electronic interaction' means an intentional and unauthorized attempt to cause a safety or other negative impact on aircraft operations by—

''(A) modifying an aeronautical database;

''(B) corrupting software; or

''(C) accessing an aircraft or aeronautical system using an internet connection or other form of electronic connection.

''(8) NATIONAL AIRSPACE SYSTEM CYBER ENVIRONMENT.—The term 'national airspace system cyber environment' means the networking and computing technology infrastructures and data used to perform air navigation services (including air traffic control and air traffic management services), including the internet, telecommunications networks, com-

puter systems, and embedded processors and controllers.''.

(b) CLERICAL AMENDMENT.—The analysis for chapter 401 of title 49, United States Code, is amended by adding at the end the following:

''40131. National airspace system cyber threat management process.''.

SEC. 7. CIVIL AIRCRAFT CYBERSECURITY AVIATION RULEMAKING COMMITTEE.

(a) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Administrator of the Federal Aviation Administration shall convene an aviation rulemaking committee on civil aircraft cybersecurity to conduct a review and develop findings and recommendations on cybersecurity standards for civil aircraft, aircraft ground support information systems, and aeronautical products and articles.

(b) DUTIES.—The Administrator shall—

(1) not later than 2 years after the date of enactment of this Act, submit to Congress a report based on the findings of the aviation rulemaking committee convened under subsection (a); and

(2) not later than 180 days after the date of submission of the report under paragraph (1), issue a notice of proposed rulemaking based on any consensus recommendations reached by such committee.

(c) COMPOSITION.—The aviation rulemaking committee convened under subsection (a) shall consist of members appointed by the Administrator, including representatives of—

(1) aircraft manufacturers;

(2) air carriers;

(3) the Federal Aviation Administration;

(4) such Federal agencies as the Administrator considers appropriate; and

(5) aviation safety experts with specific knowledge of aircraft cybersecurity.

(d) MEMBER ACCESS TO SENSITIVE SECURITY INFORMATION.—Not later than 60 days after the date of a member's appointment under subsection (c), the Administrator shall determine if there is cause for the member to be restricted from possessing sensitive security information. Upon a determination of no cause being found regarding the member, and upon the member voluntarily signing a nondisclosure agreement, the member may be granted access to sensitive security information that is relevant to the member's duties on the aviation rulemaking committee. The member shall protect the sensitive security information in accordance with part 1520 of title 49, Code of Federal Regulations.

(e) PROHIBITION ON COMPENSATION.—The members of the aviation rulemaking committee convened under subsection (a) shall not receive pay, allowances, or benefits from the Government by reason of their service on such committee.

(f) CONSIDERATIONS.—The Administrator shall direct such committee to consider—

(1) existing cybersecurity standards, regulations, policies, and guidance, including those from other Federal agencies;

(2) threat- and risk-based security approaches used by the aviation industry, including the assessment of the potential costs and benefits of cybersecurity actions;

(3) data gathered from cybersecurity reporting;

(4) data gathered from safety reporting;

(5) the need to accommodate the diversity of operations and systems on aircraft and amongst air carriers;

(6) the need to harmonize or deconflict proposed and existing standards, regulations, policies, and guidance with other Federal standards, regulations, policies, and guidance;

(7) design approval holder aircraft network security guidance for operators;

(8) the need for such standards, regulations, policies, and guidance as applied to civil aircraft information, data, networks, systems, services, operations, and technology;

(9) updates needed to airworthiness regulations and systems safety assessment methods used to show compliance with airworthiness requirements for design, function, installation, and certification of civil aircraft, aeronautical products and articles, and aircraft networks;

(10) updates needed to air carrier operating and maintenance regulations to ensure continued adherence with processes and procedures established in airworthiness regulations to provide cybersecurity protections for aircraft systems, including for continued airworthiness;

(11) policies and procedures to coordinate with other Federal agencies, including intelligence agencies, and the aviation industry in sharing information and analyses related to cyber threats to civil aircraft information, data, networks, systems, services, operations, and technology and aeronautical products and articles;

(12) the response of the Administrator and aviation industry to, and recovery from, cyber inci-

dents, including by coordinating with other Federal agencies, including intelligence agencies;

(13) processes for members of the aviation industry to voluntarily report to the Federal Aviation Administration cyber incidents that may affect aviation safety in a manner that protects trade secrets and sensitive business information;

(14) the unique nature of the aviation industry, including aircraft networks, aircraft systems, and aeronautical products, and the interconnectedness of cybersecurity and aviation safety;

(15) appropriate cybersecurity controls for aircraft networks, aircraft systems, and aeronautical products and articles to protect aviation safety, including airworthiness;

(16) minimum standards for protecting civil aircraft, aeronautical products and articles, aviation networks, aviation systems, services, and operations from cyber threats and cyber incidents;

(17) international collaboration, where appropriate and consistent with the interests of aviation safety in air commerce and national security, with other civil aviation authorities, international aviation and standards organizations, and any other appro-

priate entities to protect civil aviation from cyber incidents and cyber threats;

(18) the recommendations and implementation of the Aircraft System Information Security/Protection report of the aviation rulemaking advisory committee submitted on August 22, 2022; and

(19) any other matter the Administrator determines appropriate.

(g) DEFINITIONS.—The definitions set forth in section 40131 of title 49, United States Code (as added by this Act), apply to this section.

○