(1) ACCESS TO INFORMATION.—The Administrator of the Federal Aviation Administration, for certification purposes of the Administration only, is authorized—

(A) to conduct, in accordance with the established request process, a criminal history background check of an airman in the criminal repositories of the Federal Bureau of Investigation and States by submitting positive identification of the airman to a fingerprint-based repository in compliance with section 217 of the National Crime Prevention and Privacy Compact Act of 1998 (34 U.S.C. 40316); and

(B) to receive relevant criminal history record information regarding the airman checked.

(2) RELEASE OF INFORMATION.—In accessing a repository referred to in paragraph (1), the Administrator shall be subject to the conditions and procedures established by the Department of Justice or the State, as appropriate, for other governmental agencies conducting background checks for noncriminal justice purposes.

(3) LIMITATION.—The Administrator may not use the authority under paragraph (1) to conduct criminal investigations.

(4) REIMBURSEMENT.—The Administrator may collect reimbursement to process the fingerprint-based checks under this subsection, to be used for expenses incurred, including Federal Bureau of Investigation fees, in providing these services.

(b) DESIGNATED EMPLOYEES.—The Administrator shall designate, by order, employees of the Administration who may carry out the authority described in subsection (a).

(Added Pub. L. 112–95, title VIII, §802(a), Feb. 14, 2012, 126 Stat. 118; amended Pub. L. 118–63, title XI, §1101(h), May 16, 2024, 138 Stat. 1413.)

Editorial Notes

AMENDMENTS

2024—Subsec. (a)(1)(A). Pub. L. 118–63 substituted ''(34 U.S.C. 40316)'' for ''(42 U.S.C. 14616)''.

§ 40131. National airspace system cyber threat management process

(a) ESTABLISHMENT.—The Administrator of the Federal Aviation Administration, in consultation with the heads of other agencies as the Administrator determines necessary, 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 air navigation 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 for significant cybersecurity incidents;

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

(6) track significant cyber incident detection, response, mitigation implementation, recovery, and closure;

(7) establish a process, or utilize existing processes, to share relevant significant cyber incident data related to the national airspace system;

(8) facilitate significant cybersecurity reporting, including through the Cybersecurity and Infrastructure Agency; and

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

(c) DEFINITIONS.—In this section:

(1) 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.

(2) 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.

(3) CYBER INCIDENT.—The term ''cyber incident'' means an action that creates noticeable degradation, disruption, or destruction to the cyber environment and causes a safety or other negative impact on operations of—

(A) the national airspace system;

(B) civil aircraft; or

(C) aeronautical products and articles.

(4) CYBER THREAT.—The term ''cyber threat'' means the threat of an action that, if carried out, would constitute a cyber incident or an electronic attack.

(5) 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.

(6) SIGNIFICANT CYBER INCIDENT.—The term ''significant cyber incident'' means a cyber incident, or a group of related cyber incidents, that the Administrator determines is likely to result in demonstrable harm to the national airspace system of the United States.

(Added Pub. L. 118–63, title III, §393(a), May 16, 2024, 138 Stat. 1144.)

Statutory Notes and Related Subsidiaries

CYBERSECURITY LEAD

Pub. L. 118–63, title II, §217, May 16, 2024, 138 Stat. 1055, provided that:

''(a) IN GENERAL.—The Administrator [of the Federal Aviation Administration] shall designate an executive

of the FAA [Federal Aviation Administration] to serve as the lead for the cybersecurity of FAA systems and hardware (in this section referred to as the 'Cybersecurity Lead').

''(b) DUTIES.—The Cybersecurity Lead shall carry out duties and powers prescribed by the Administrator, including the management of activities required under subtitle B of title III.

''(c) BRIEFING.—Not later than 1 and 3 years after the date of enactment of this Act [May 16, 2024], the Cybersecurity Lead shall brief the appropriate committees of Congress on the implementation of subtitle B of title III.''

CIVIL AVIATION CYBERSECURITY RULEMAKING COMMITTEE

Pub. L. 118–63, title III, § 395, May 16, 2024, 138 Stat. 1145, provided that:

''(a) IN GENERAL.—Not later than 1 year after the date of enactment of this Act [May 16, 2024], the Administrator [of the Federal Aviation Administration] shall convene an aviation rulemaking committee on civil aircraft cybersecurity to conduct reviews (as segmented under subsection (c)) and develop findings and recommendations on cybersecurity standards for civil aircraft, aircraft ground support information systems, airports, air traffic control mission systems, and aeronautical products and articles.

''(b) DUTIES.—The Administrator shall—

''(1) for each segmented review conducted by the committee convened under subsection (a), submit to the appropriate committees of Congress a report based on the findings of such review; and

''(2) not later than 180 days after the date of submission of a report under paragraph (1) and, in consultation with other agencies as the Administrator determines necessary, for consensus recommendations reached by such aviation rulemaking committee—

''(A) undertake a rulemaking, if appropriate, based on such recommendations; and

''(B) submit to the appropriate committees of Congress a supplemental report with explanations for each consensus recommendation not addressed, if applicable, by a rulemaking under subparagraph (A).

''(c) SEGMENTATION.—In tasking the aviation rulemaking committee with developing findings and recommendations relating to aviation cybersecurity, the Administrator shall direct such committee to segment and sequence work by the topic or subject matter of regulation, including by directing the committee to establish subgroups to consider different topics and subject matters.

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

''(1) aircraft manufacturers, to include at least 1 manufacturer of transport category aircraft;

''(2) air carriers;

''(3) unmanned aircraft system stakeholders, including operators, service suppliers, and manufacturers of hardware components and software applications;

''(4) manufacturers of powered-lift aircraft;

''(5) airports;

''(6) original equipment manufacturers of ground and space-based aviation infrastructure;

''(7) aviation safety experts with specific knowledge of aircraft cybersecurity; and

''(8) a nonprofit which operates 1 or more federally funded research and development centers with specific knowledge of aviation and cybersecurity.

''(e) MEMBER ELIGIBILITY.—Prior to a member's appointment under subsection (c) [probably should be ''subsection (d)''], the Administrator shall establish appropriate requirements related to nondisclosure, background investigations, security clearances, or other screening mechanisms for applicable members of the aviation rulemaking committee who require access to sensitive security information or other protected information relevant to the member's duties on the rulemaking committee. Members shall protect the sensitive security information in accordance with part 1520 of title 49, Code of Federal Regulations.

''(f) 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.

''(g) CONSIDERATIONS.—The Administrator may direct such committee to consider—

''(1) existing aviation cybersecurity standards, regulations, policies, and guidance, including those from other Federal agencies, and the need to harmonize or deconflict proposed and existing standards, regulations, policies, and guidance;

''(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 or safety reporting;

''(4) the diversity of operations and systems on aircraft and amongst air carriers;

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

''(6) FAA services, aviation industry services, and aircraft use of positioning, navigation, and timing data in the context of Executive Order No. 13905 [6 U.S.C. 651 note], as in effect on the date of enactment of this Act;

''(7) 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;

''(8) 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;

''(9) 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;

''(10) the response of the Administrator and aviation industry to, and recovery from, cyber incidents, including by coordinating with other Federal agencies, including intelligence agencies;

''(11) processes for members of the aviation industry to voluntarily report to the FAA cyber incidents that may affect aviation safety in a manner that protects trade secrets and confidential business information;

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

''(13) appropriate cybersecurity controls for airports relative to the size and nature of airside operations of such airports to ensure aviation safety;

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

''(15) 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 appropriate entities to protect civil aviation from cyber incidents and cyber threats;

''(16) activities of the Administrator under section 506 of the FAA Reauthorization Act of 2018 [Pub. L.

115–254] (49 U.S.C. 44704 note) (as amended by section 394); and

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

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

§ 40132. National strategic plan for aviation workforce development

(a) IN GENERAL.—Not later than September 30, 2025, the Secretary of Transportation shall, in consultation with other Federal agencies and the Cooperative Aviation Recruitment, Enrichment, and Employment Readiness Council (in this section referred to as the ''CAREER Council'') established in subsection (c), establish and maintain a national strategic plan to improve recruitment, hiring, and retention and address projected challenges in the civil aviation workforce, including—

(1) any short-term, medium-term, and long-term workforce challenges relevant to the economy, workforce readiness, and priorities of the United States aviation sector;

(2) any existing or projected workforce shortages; and

(3) any workforce situation or condition that warrants special attention by the Federal Government.

(b) REQUIREMENTS.—The national strategic plan described in subsection (a) shall—

(1) take into account the activities and accomplishments of all Federal agencies that are related to carrying out such plan;

(2) include recommendations for carrying out such plan; and

(3) project and identify, on an annual basis, aviation workforce challenges, including any applicable workforce shortages.

(c) CAREER COUNCIL.—

(1) ESTABLISHMENT.—Not later than September 30, 2025, the Secretary, in consultation with the Administrator, shall establish a council comprised of individuals with expertise in the civil aviation industry to—

(A) assist with developing and maintaining the national strategic plan described in subsection (a); and

(B) provide advice to the Secretary, as appropriate, relating to the CAREER Program established under section 625 of the FAA Reauthorization Act of 2018, including as such advice relates to program administration and grant application selection, and support the development of performance metrics regarding the quality and outcomes of the Program.

(2) APPOINTMENT.—The CAREER Council shall be appointed by the Secretary from candidates nominated by national associations representing various sectors of the aviation industry, including—

(A) commercial aviation;

(B) general aviation;

(C) aviation labor organizations, including collective bargaining representatives of Federal Aviation Administration aviation safety inspectors, aviation safety engineers, and air traffic controllers;

(D) aviation maintenance, repair, and overhaul;

(E) aviation manufacturers; and

(F) unmanned aviation.

(3) TERM.—Each council member appointed by the Secretary under paragraph (2) shall serve a term of 2 years.

(d) NONDELEGATION.—The Secretary may not delegate any of the authorities or responsibilities under this section to the Administrator of the Federal Aviation Administration.

(Added Pub. L. 118–63, title IV, § 441(a), May 16, 2024, 138 Stat. 1184.)

Editorial Notes

REFERENCES IN TEXT

Section 625 of the FAA Reauthorization Act of 2018, referred to in subsec. (c)(1)(B), is section 625 of Pub. L. 115–254, which is set out as a note below.

Statutory Notes and Related Subsidiaries

PILOT PROGRAM TO PROVIDE VETERANS WITH PILOT TRAINING SERVICES

Pub. L. 118–63, title IV, § 418, May 16, 2024, 138 Stat. 1162, provided that:

''(a) IN GENERAL.—The Secretary [of Transportation], in consultation with the Secretary of Education and the Secretary of Veterans Affairs, shall establish a pilot program to provide grants to eligible entities to provide pilot training activities and related education to support a pathway for veterans to become commercial aviators.

''(b) ELIGIBLE ENTITY.—In this section, the term 'eligible entity' means a pilot school or provisional pilot school that—

''(1) holds an Air Agency Certificate under part 141 of title 14, Code of Federal Regulations; and

''(2) has an established employment pathway with at least 1 air carrier operating under part 121 or 135 of title 14, Code of Federal Regulations.

''(c) PRIORITY APPLICATION.—In selecting eligible entities under this section, the Secretary shall prioritize eligible entities that meet the following criteria:

''(1) An eligible entity accredited (as defined in section 61.1 of title 14, Code of Federal Regulations) by an accrediting agency recognized by the Secretary of Education.

''(2) An eligible entity that holds a letter of authorization issued in accordance with section 61.169 of title 14, Code of Federal Regulations.

''(d) USE OF FUNDS.—Amounts from a grant received by an eligible entity under the pilot program established under subsection (a) shall be used for the following:

''(1) Administrative costs related to implementation of the program described in subsection (a) not to exceed 5 percent of the amount awarded.

''(2) To provide guidance and pilot training services, including tuition and flight training fees for veterans enrolled with an eligible entity, to support such veterans in obtaining any of the following pilot certificates and ratings:

''(A) Private pilot certificate with airplane single-engine or multi-engine ratings.

''(B) Instrument rating.

''(C) Commercial pilot certificate with airplane single-engine or multi-engine ratings.

''(D) Multi-engine rating.

''(E) Certificated flight instructor single-engine certificate, if applicable to the degree sought.

''(F) Certificated flight instructor multi-engine certificate, if applicable to the degree sought.

''(G) Certificated flight instructor instrument certificate, if applicable to the degree sought.