

(2) VIEWS.—The Administrator may obtain the views of interested parties in issuing the guidelines.

(d) EFFECT OF DETERMINATION OF EXISTENCE OF CAPACITY REDUCTION EVENT.—Upon a determination by the Administrator that a capacity reduction event exists, the Administrator may authorize air carriers and foreign air carriers operating at an airport participating in the pilot program to communicate for a period of time not to exceed 24 hours with each other concerning changes in their respective flight schedules in order to use air traffic capacity most effectively. The Administration shall facilitate and monitor such communication. The Attorney General, or the Attorney General's designee, may monitor such communication.

(e) SELECTION OF PARTICIPATING AIRPORTS.—Not later than 30 days after the date on which the Administrator establishes the pilot program, the Administrator shall select 2 airports to participate in the pilot program from among the most capacity-constrained airports in the Nation based on the Administration's Airport Capacity Benchmark Report 2001 or more recent data on airport capacity that is available to the Administrator. The Administrator shall select an airport for participation in the pilot program if the Administrator determines that collaborative decisionmaking among air carriers and foreign air carriers would reduce delays at the airport and have beneficial effects on reducing delays in the national airspace system as a whole.

(f) ELIGIBILITY OF AIR CARRIERS.—An air carrier or foreign air carrier operating at an airport selected to participate in the pilot program is eligible to participate in the pilot program if the Administrator determines that the carrier has the operational and communications capability to participate in the pilot program.

(g) MODIFICATION OR TERMINATION OF PILOT PROGRAM AT AN AIRPORT.—The Administrator, with the concurrence of the Attorney General, may modify or end the pilot program at an airport before the term of the pilot program has expired, or may ban an air carrier or foreign air carrier from participating in the program, if the Administrator determines that the purpose of the pilot program is not being furthered by participation of the airport or air carrier or if the Secretary of Transportation, with the concurrence of the Attorney General, finds that the pilot program or the participation of an air carrier or foreign air carrier in the pilot program has had, or is having, an adverse effect on competition among carriers.

(h) ANTITRUST IMMUNITY.—

(1) IN GENERAL.—Unless, within 5 days after receiving notice from the Secretary of the Secretary's intention to exercise authority under this subsection, the Attorney General submits to the Secretary a written objection to such action, including reasons for such objection, the Secretary may exempt an air carrier's or foreign air carrier's activities that are necessary to participate in the pilot program under this section from the antitrust laws for the sole purpose of participating in the pilot program. Such exemption shall not extend to any discussions, agreements, or activities outside the scope of the pilot program.

(2) ANTITRUST LAWS DEFINED.—In this section, the term "antitrust laws" has the meaning given that term in the first section of the Clayton Act (15 U.S.C. 12).

(i) CONSULTATION WITH ATTORNEY GENERAL.—The Secretary shall consult with the Attorney General regarding the design and implementation of the pilot program, including determining whether a limit should be set on the number of occasions collaborative decisionmaking could be employed during the initial 2-year period of the pilot program.

(j) EVALUATION.—

(1) IN GENERAL.—Before the expiration of the 2-year period for which the pilot program is authorized under subsection (b), the Administrator shall determine whether the pilot program has facilitated more effective use of air traffic capacity and the Secretary, with the concurrence of the Attorney General, shall determine whether the pilot program has had an adverse effect on airline competition or the availability of air services to communities. The Administrator shall also examine whether capacity benefits resulting from the participation in the pilot program of an airport resulted in capacity benefits to other parts of the national airspace system.

(2) OBTAINING NECESSARY DATA.—The Administrator may require participating air carriers and airports to provide data necessary to evaluate the pilot program's impact.

(k) EXTENSION OF PILOT PROGRAM.—At the end of the 2-year period for which the pilot program is authorized, the Administrator, with the concurrence of the Attorney General, may continue the pilot program for an additional 2 years and expand participation in the program to up to 7 additional airports if the Administrator determines pursuant to subsection (j) that the pilot program has facilitated more effective use of air traffic capacity and if the Secretary, with the concurrence of the Attorney General, determines that the pilot program has had no adverse effect on airline competition or the availability of air services to communities. The Administrator shall select the additional airports to participate in the extended pilot program in the same manner in which airports were initially selected to participate.

(Added Pub. L. 108-176, title IV, § 423(a), Dec. 12, 2003, 117 Stat. 2552.)

Editorial Notes

REFERENCES IN TEXT

The date of enactment of this section, referred to in subsec. (a), is the date of enactment of Pub. L. 108-176, which was approved Dec. 12, 2003.

Statutory Notes and Related Subsidiaries

EFFECTIVE DATE

Section applicable only to fiscal years beginning after Sept. 30, 2003, except as otherwise specifically provided, see section 3 of Pub. L. 108-176, set out as an Effective Date of 2003 Amendment note under section 106 of this title.

§ 40130. FAA authority to conduct criminal history record checks

(a) CRIMINAL HISTORY BACKGROUND CHECKS.—

(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