U.S. Department
of Transportation
**Federal Aviation
Administration**

Effective Date: 05/13/25

SUBJECT: Civil Aviation Cybersecurity Aviation Rulemaking Committee

---

1. **PURPOSE.** This charter establishes the Civil Aviation Cybersecurity Aviation Rulemaking Committee (ARC), according to the Administrator's authority under Title 49 of the United States Code (49 U.S.C. § 106(p)(5)) and as mandated by the Federal Aviation Administration (FAA) Reauthorization Act of 2024, Public Law 118-63 (the Act). The sponsor of the ARC is the FAA's Chief Information Security Officer (CISO). This charter outlines the ARC's organization, responsibilities, and tasks.

2. **BACKGROUND.** Section 395 of the Act directs the FAA to convene the Civil Aviation Cybersecurity ARC by May 15, 2025, to review 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.

3. **OBJECTIVES OF THE ARC.** The Civil Aviation Cybersecurity ARC will provide a forum for the appointed members to conduct reviews, discuss, and provide findings and recommendations to the FAA focused on cybersecurity standards for civil aircraft, aircraft ground support information systems, airports, air traffic control mission systems, and aeronautical products and articles.

4. **TASKS OF THE ARC.** The tasks of the ARC are as follows:

   a. Determine whether cybersecurity-related rulemaking, policies, and guidance are recommended for the product type design and production processes, including the development of Instructions for Continued Airworthiness. In developing findings and recommendations, the ARC will consider:

      i. minimum standards for protecting civil aircraft and aeronautical products and articles from cyber threats and cyber incidents;

      ii. whether updates are 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;

      iii. appropriate cybersecurity controls for aircraft networks, aircraft systems, and aeronautical products and articles to protect aviation safety, including airworthiness; and

      iv. design approval holder aircraft network security guidance for operators.

b. Determine whether cybersecurity-related rulemaking, policies, and guidance are recommended to address the in-service operation, maintenance, and support stages of the civil aircraft life cycle. In developing findings and recommendations, the ARC will consider:

   i. the diversity of operations and systems on aircraft and amongst air carriers, including aircraft not certified under special conditions related to Aircraft Systems Information Security Protection, and for which an Aircraft Information Security Program has not been developed;

   ii. whether updates are needed to air carrier operating and maintenance regulations to ensure continued adherence with processes and procedures established in airworthiness regulations and standards to provide cybersecurity protections for aircraft systems, including for continued airworthiness; and

   iii. minimum capabilities required of aircraft flight crews to maintain aircraft safety during a cyber incident affecting navigation and other aircraft systems while the aircraft is in operation.

c. Determine whether and how aviation cybersecurity or safety reporting can be confidentially reported to the FAA, incorporated into aviation-specific cybersecurity risk assessment methodologies, and the resulting analyses shared with other federal agencies and the aviation industry, in order to prevent, respond to, and recover from cyber threats and cyber incidents. In developing findings and recommendations, the ARC will consider:

   i. data gathered from cybersecurity or safety reporting;

   ii. 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;

   iii. 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; and

   iv. the Administrator and the aviation industry's response to, and recovery from, cyber incidents, including coordination with other federal agencies, including intelligence agencies.

d. Determine whether existing or proposed cybersecurity standards, regulations, policies, guidance, and threat- and risk-based security approaches should be harmonized with those of other federal agencies, other civil aviation authorities, and international aviation and standards organizations. In developing findings and recommendations, the ARC will consider:

i. 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;

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

iii. appropriate processes to identify and manage cybersecurity risks within aviation organizations, including those from the supply chain, that could affect safety in air commerce, including operations at airports and throughout the design, production, operations, and maintenance lifecycle of the aircraft; and

iv. 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.

e. Determine whether cybersecurity-related rulemaking, policies, guidance, or minimum standards are recommended to protect aviation systems, services, and operations from cyber threats and cyber incidents. In developing findings and recommendations, the ARC will consider:

i. emerging technologies and applications, such as artificial intelligence and machine learning;

ii. levels of automation and autonomy within the context of diverse operations; and

iii. third-party providers of services.

f. Determine whether cybersecurity-related rulemaking, policies, and/or guidance are recommended to identify appropriate cybersecurity controls for airports relative to the size and nature of airside operations of such airports to ensure aviation safety.

g. Consider any other matter the Administrator determines appropriate.

h. Provide rationale as to why or why not cybersecurity-related rulemaking, policy, or guidance is required for Tasks 4a. through 4g., and if rulemaking is recommended, specify where in the current regulatory framework such rulemaking would be placed.

i. If it is recommended that cybersecurity-related policy and guidance on best practices is needed, recommend whether security-related industry standards from Aeronautical Radio Incorporated, Federal Information Processing Standards, International Standards Organization, National Institute of Standards and Technology, RTCA, Inc., Society of Automotive Engineers, or American Society for Testing and Materials International would be appropriate for use in such cybersecurity-related policy and/or guidance.

j. If recommending cybersecurity-related rulemaking, provide quantitative benefit and cost estimates, qualitative benefit-cost description, and compliance trade-offs for any rulemaking recommendation.

k. Within 18 months from the first meeting after the effective date of the charter, submit recommendations for each segmented review organized into reports as determined collaboratively by the FAA Co-Chair and Industry Co-Chairs.

i. The recommendation reports should document both majority and dissenting positions on the findings and the rationale for each position. Any disagreements should be documented, including the rationale for each position and the reasons for disagreement.

ii. The Industry Co-Chairs send the recommendation reports to the FAA Co-Chair and the Executive Director of the Office of Rulemaking.

iii. The FAA Co-Chair determines when the recommendation reports and records, pursuant to paragraph (8), will be made available for public release.

iv. Within 6 months of the first meeting of the ARC after the effective date of this charter, and every 6 months thereafter, submit interim reports to the Sponsor.

5. ARC PROCEDURES.

a. The ARC acts solely in an advisory capacity by advising and providing written recommendations to the FAA Co-Chair.

b. The ARC may propose related follow-on tasks outside the stated scope of the ARC to the FAA Co-Chair.

c. The ARC may reconvene following the submission of the recommendation report for the purposes of providing advice and assistance to the FAA, at the discretion of the FAA Co-Chair, provided the Charter is still in effect.

6. ARC ORGANIZATION, MEMBERSHIP, AND ADMINISTRATION. As prescribed in Section 395, paragraph (d) of the Act, the ARC membership will include representatives from the following aviation stakeholders:

a. aircraft manufacturers, including at least one manufacturer of transport category aircraft;

b. air carriers;

c. unmanned aircraft system stakeholders, including operators, service suppliers, and manufacturers of hardware components and software applications;

d. manufacturers of powered-lift aircraft;

e. airports;

f. original equipment manufacturers of ground- and space-based aviation infrastructure;

g. aviation safety experts with specific knowledge of aircraft cybersecurity; and

h. a non-profit that operates one or more federally funded research and development centers with specific knowledge of aviation cybersecurity.

Members will be selected based on their subject matter expertise in aviation cybersecurity and their familiarity with the FAA's authorities, existing regulations, and guidance related to aviation cybersecurity. Membership will be balanced in viewpoints and interests. All members should have knowledge of the ARC's objectives and scope.

As prescribed in Section 395, paragraph (e), the FAA will establish appropriate requirements related to nondisclosure, background investigations, security clearances, or other screening mechanisms for applicable members of the ARC who require access to sensitive security information or other protected information relevant to their duties on the ARC. Membership on the ARC is contingent upon agreeing to the established requirements.

Members will not receive pay, allowances, or benefits from the Federal Government by reason of their service on this committee.

The provisions of the August 13, 2014, Office of Management and Budget (OMB) guidance, "Revised Guidance on Appointment of Lobbyists to Federal Advisory Committees, Boards, and Commissions" (79 FR 47482), continues the ban on registered lobbyists participating on Agency Boards and Commissions if participating in their "individual capacity." The revised guidance allows registered lobbyists to participate on Agency Boards and Commissions in a "representative capacity" for the "express purpose of providing a committee with the views of a nongovernmental entity, a recognizable group of persons or nongovernmental entities (an industry, sector, labor unions, or environmental groups, etc.) or state or local government." For further information, refer to the OMB Guidance at 79 FR 47482.

Membership is limited to promote discussion. Attendance, active participation, and commitment by members are essential for achieving the objectives and tasks. In general, members will be appointed for the duration of the ARC. When necessary, the ARC may set up specialized and temporary working groups that include at least one ARC member and invited subject matter experts from industry and government.

Other Federal Government agency subject matter experts may be requested to participate as Observers and to provide technical support to the ARC members.

a. The Sponsor, the CISO, will designate the FAA Co-Chair who will:

    1) select and appoint industry members and the FAA participants;

2) select the Industry Co-Chairs from the membership of the ARC;

3) determine, in collaboration with the Industry Co-Chairs, how to segment and sequence work by the topic or subject matter of regulation and establish subgroups to consider different topics and subject matters;

4) ensure appropriate FAA participation and support from all affected Lines of Business and Staff Offices;

5) provide notification to the members of the time and place for each meeting, and

6) receive any status and recommendations reports.

b. Once appointed, the Industry Co-Chairs will:

1) coordinate required ARC meetings in order to meet the objectives and timelines;

2) establish and distribute meeting agendas in a timely manner;

3) keep meeting notes, if deemed necessary;

4) perform other responsibilities as required to ensure the objectives are met;

5) provide status reports, as requested, in writing to the FAA Co-Chair, and

6) submit the recommendation report to the FAA Co-Chair and the Executive Director of the Office of Rulemaking.

7. PUBLIC PARTICIPATION. Meetings are not open to the public. Persons or organizations outside the ARC who wish to attend a meeting must get approval in advance of the meeting from the Industry Co-Chairs and the FAA Co-Chair.

8. AVAILABILITY OF RECORDS. Subject to applicable Freedom of Information Act Exemptions pursuant to Title 5, U.S.C., § 552, the FAA will make records provided by the ARC to the FAA available for public inspection and copying. Available records will be located at the Information Security and Privacy Office, FAA Headquarters, 800 Independence Ave. S.W., Washington, D.C., 20591. Fees will be charged for information furnished to the public according to the fee schedule published in Title 49 of the Code of Federal Regulations, Part 7.

You can find this charter on the FAA Committee Database website at:
http://www.faa.gov/regulations_policies/rulemaking/committees/documents/

9. DISTRIBUTION. This charter is distributed to the Office of the Assistant Administrator for Finance and Management; the Office of the Associate Administrator for Aviation Safety; the Office of the Associate Administrator for Airports; the Office of the Associate Administrator for Commercial Space Transportation; the Office of the Associate Administrator for Security and

Hazardous Materials; the Office of the Chief Operating Officer, Air Traffic Organization; Office of the Assistant Administrator for NextGen; the Office of the Chief Counsel; the Office of the Assistant Administrator for Policy, International Affairs, and Environment; and the Office of Rulemaking.

10. EFFECTIVE DATE AND DURATION. The ARC is effective upon issuance of this charter and will remain in existence for a maximum of 2 years unless the Administrator suspends, terminates, or extends the charter earlier.

Issued in Washington, D.C. on May 13, 2025

Christopher J. Rocheleau

Christopher J. Rocheleau
Acting Administrator