BILLING CODE 4910-13-P

DEPARTMENT OF TRANSPORTATION

Federal Aviation Administration

14 CFR Parts 25, 33, and 35

[Docket No.: FAA-2024-1398; Notice No. 24-23]

RIN 2120-AL94

Equipment, Systems, and Network Information Security Protection

AGENCY: Federal Aviation Administration (FAA), Department of Transportation (DOT).

ACTION: Notice of proposed rulemaking.

SUMMARY: This proposed rulemaking would impose new design standards to address cybersecurity threats for transport category airplanes, engines, and propellers. The intended effect of this proposed action is to standardize the FAA's criteria for addressing cybersecurity threats, reducing certification costs and time while maintaining the same level of safety provided by current special conditions.

DATES: Send comments on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Send comments identified by docket number FAA-2024-1398 using any of the following methods:

- Federal eRulemaking Portal: Go to www.regulations.gov and follow the online instructions for sending your comments electronically.
- Mail: Send comments to Docket Operations, M-30; U.S. Department of Transportation, 1200 New Jersey Avenue, SE, Room W12-140, West Building Ground Floor, Washington, DC 20590-0001.
- Hand Delivery or Courier: Take comments to Docket Operations in Room W12-140 of the West Building Ground Floor at 1200 New Jersey Avenue, SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.
- Fax: Fax comments to Docket Operations at (202) 493-2251.

Privacy: In accordance with 5 U.S.C. 553(c), DOT solicits comments from the public to better inform its rulemaking process. DOT posts these comments, without edit, including any personal information the commenter provides, to www.regulations.gov, as described in the system of records notice (DOT/ALL-14 FDMS), which can be reviewed at www.dot.gov/privacy.

Docket: Background documents or comments received may be read at www.regulations.gov at any time. Follow the online instructions for accessing the docket or go to the Docket Operations in Room W12-140 of the West Building Ground Floor at 1200 New Jersey Avenue, SE, Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays.

FOR FURTHER INFORMATION CONTACT: For technical questions concerning this action, contact Varun Khanna, AIR-626D, Policy and Standards Division, Aircraft

Certification Service, Federal Aviation Administration, 2200 South 216th Street, Des Moines, WA 98198; telephone (206) 231 3159; e-mail varun.khanna@faa.gov.

SUPPLEMENTARY INFORMATION:

I. Executive Summary

A. Overview of Proposed Rule

The FAA proposes to add new regulations to and revise certain existing regulations in title 14, Code of Federal Regulations (14 CFR) part 25 (Airworthiness Standards: Transport Category Airplanes), part 33 (Airworthiness Standards: Aircraft Engines), and part 35 (Airworthiness Standards: Propellers). These changes would introduce type certification and continued airworthiness requirements to protect the equipment, systems, and networks of transport category airplanes, engines, and propellers against intentional unauthorized electronic interactions (IUEI)[1] that could create safety hazards. Design approval applicants would be required to identify, assess, and mitigate such hazards, and develop Instructions for Continued Airworthiness (ICA) that would ensure such protections continue in service. Proposed changes to parts 25, 33, and 35 would mandate such protection and apply to applicants for design approval of transport category airplanes, engines, and propellers. The changes would also affect future operators of these products through the application of the ICA.

---

[1] RTCA Glossary page 24: Intentional Unauthorized Electronic Interaction (IUEI) is defined, for purposes of this rulemaking, as "[a] circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. Note that this includes malware and the effects of external systems, but does not include physical attacks such as electromagnetic jamming."

The substance of the proposed rules would generally reflect current practice (e.g., special conditions) that the FAA has used to address product cybersecurity since 2009. Under the proposed regulations, the FAA would continue to apply the same substantive requirements established by current special conditions via the same methods of compliance to new applicable certification projects; thus, the impact on applicants and operators would not be significant. The intended effect of this action is to reduce the costs and time necessary to certify new and changed products and harmonize FAA regulatory requirements with the regulations that other civil aviation authorities are using to address cybersecurity vulnerability, while maintaining the level of safety provided by current Aircraft System Information Security/Protection (ASISP) special conditions.

B. Background

The current trend in airplane design includes an increasing level of integration of airplane, engine, and propeller systems with increased connectivity to internal or external data networks and services. Regulators and industry must constantly monitor the cybersecurity threat environment in order to identify and mitigate new threat sources. These designs can introduce or allow cybersecurity vulnerabilities from sources such as:

- Field Loadable Software;
- Maintenance laptops;
- Airport or airline gate link networks;
- Public networks, e.g., Internet;
- Wireless aircraft sensors and sensor networks;
- Cellular networks;

- Universal Serial Bus (USB) devices;
- Satellite communications;
- Portable electronic devices and portable electronic flight bags (EFBs); and
- GPS and satellite-based augmentation system digital data.

The FAA has found its airworthiness regulations, including §§ 25.1301, 25.1309, 25.1319, 25.1529, 33.28, and 35.23, inadequate and inappropriate to address the cybersecurity vulnerabilities caused by increased interconnectivity. Beginning with the Boeing 787 program, the FAA has been addressing the need to protect aircraft systems from the threat of IUEI. Since then, the FAA has issued special conditions to address IUEI in every new transport category airplane certification project and relevant design change. A special condition is a rule that applies to a particular aircraft, aircraft engine, or propeller design. The FAA issues special conditions when the agency's airworthiness regulations do not contain adequate or appropriate safety standards to address a proposed novel or unusual design feature. The FAA provides the public with an opportunity to comment on proposed special conditions.[2]

Each set of special conditions addresses a project-specific novel or unusual feature of the applicant's proposed design. The FAA's special conditions addressing cybersecurity on transport category airplanes have generally required applicants' proposed designs to accomplish three things. Applicants have been required to:

---

[2] 14 CFR 21.16.

1. Show that their proposed airplane designs either provide isolation from or protection against internal or external unauthorized access.
2. Show that their designs prevent inadvertent changes, malicious changes, and all adverse impacts to the airplane equipment, systems, and networks necessary for safe operation.
3. Establish procedures to ensure that they maintain such cybersecurity protections.[3]

Applicants have met the first two criteria using the method of compliance (MoC) part of the cybersecurity special condition issue papers. Special conditions are issued if the existing applicable airworthiness standards do not contain adequate or appropriate safety standards for an aircraft, aircraft engine, or propeller because of novel or unusual design features of the product to be type certificated. Issue papers provide a structured means for describing and tracking the resolution of significant technical, regulatory, and administrative issues that occur during a project. The early cybersecurity MoC followed the positions listed in those issue papers: the applicants created a certification plan meeting those positions, then the FAA approved that certification plan. After RTCA, Inc. published its guidance (Document (DO)-326, DO-355, and DO-356), industry wanted to use them as a MoC.

After it became evident to the FAA that this new level of system interconnectivity would most appropriately be addressed through a single set of objective airworthiness

---

[3] See, e.g., 88 FR 46953 (July 21, 2023) and 89 FR 3333 (January 18, 2024).

standards, on December 18, 2014, the Aviation Rulemaking Advisory Committee (ARAC) accepted a task from the FAA to provide recommendations regarding ASISP[4] rulemaking, policy, and guidance on best practices for aircraft systems and parts, including both certification and continued airworthiness. ASISP refers to the protection of aircraft from electronic threats from IUEI. The ARAC created the ASISP Working Group comprised of a wide range of domestic and international industry and government experts tasked to ensure that the resulting recommendations considered relevant design, airworthiness, and international harmonization. On August 22, 2016, the working group submitted their report, including unanimous recommendations, to the ARAC. The ARAC approved and publicly released the report during its September 15, 2016 meeting.[5]

The report contained several recommendations on the necessity for ASISP-related rulemaking and guidance, including specific proposals for rule language and destination within the current regulatory framework for both type certification and continued airworthiness. This NPRM addresses the report's recommendations for the FAA to conduct rulemaking to add ASISP requirements to parts 25, 33, and 35 of title 14.[6]

---

[4] The term ASISP is used to exclude physical security issues related to individuals who could gain physical access to aircraft to cause malicious damage to the aircraft systems (e.g., improper maintenance procedures, fuel contamination, cutting wire bundles), which is addressed by other Federal agencies.

[5] See Aviation Rulemaking Advisory Committee (ARAC) Aircraft System Information Security/Protection (ASISP) working group to the Federal Aviation Administration, dated October 22, 2016, www.faa.gov/regulations_policies/rulemaking/committees/documents/media/ARACasisp-T1-20150203R.pdf.

[6] Recommendations 02, 14, and 15, respectively.

In the report, the ASISP Working Group proposed a regulatory framework that established a single set of objective airworthiness standards for all transport category airplanes. Its structure provided a clear set of discrete requirements for applicants to show compliance. Specific to this proposed rule, the ASISP Working Group recommended the following regulatory text for transport category airplanes:

> § 25.13XX Equipment, Systems, and Network Security Protection
>
> (a) Airplane equipment, systems, and networks, considered separately and in relation to other systems, must be protected from intentional unauthorized electronic interactions that may result in an adverse effect on the safety of the airplane by showing that the security risks have been identified, assessed, and mitigated as necessary.
>
> (b) When required by paragraph (a), applicants must make available procedures and instructions for continued airworthiness to ensure security protections are maintained.

The ASISP Working Group further recommended the FAA adopt similar provisions for engine control systems, propeller control systems, and to harmonize the regulatory requirement between U.S. and international regulatory authorities.[7]

---

[7] The Report also contained recommendations for addressing several other subjects, including cybersecurity concerns related to rotorcraft and small airplanes, which are not addressed in this proposed rulemaking.

On October 5, 2018, Congress enacted H.R.302 - FAA Reauthorization Act of 2018 (the "Act"). Section 506 of the Act requires the FAA to consider revising its airworthiness certification regulations to address cybersecurity by protecting aircraft systems, including engines and propellers, from unauthorized internal and external access. The Act further required the FAA to consider the recommendations of the ASISP Working Group discussed above.

Additionally, representatives of the European Union Aviation Safety Agency (EASA) participated in the ASISP Working Group for regulatory harmonization purposes and have implemented the recommendations of the ASISP Working Group to introduce cybersecurity provisions into their relevant certification specifications (CS). EASA CS prescribe the airworthiness standards for products certified by the European Union: CS-25 large aeroplanes corresponds to 14 CFR part 25 for transport category airplanes, CS-E for engines corresponds to 14 CFR part 33, and CS-P for propellers corresponds to 14 CFR part 35. Like the FAA, prior to implementing the recommendations of the ASISP Working Group, EASA had addressed the protection of aircraft systems from IUEI through the issuance of special conditions.

On February 22, 2019, EASA released NPA 2019-01, Aircraft Cybersecurity, a set of proposed amendments to CS-23, CS-25, CS-27, CS-29, CS-E, CS-ETSO, CS-P and also release their related acceptable means of compliance/guidance material. EASA Decision 2020/006/R "Aircraft cybersecurity" finalized these amendments and their guidance on July 1, 2020, issuing CS-25 Amendment 25, CS-E Amendment 6, and CS-P Amendment 2, along with amendments to CS for other product types. These amendments

introduced cybersecurity provisions into the relevant CS, incorporating the provisions of the existing EASA special conditions and the ARAC ASISP recommendations. While EASA also codified cybersecurity provisions for other product types such as small airplanes and rotorcraft, the FAA proposes no such requirements, as existing rules in parts 23 (§§ 23.2500, 23.2505, 23.2510), 27 (§§ 27.1301, 27.1309), and 29 (§§ 29.1301, 29.1309) suffice in these cases.[8]

C. Statement of the Problem

Aircraft, engines, and propellers increasingly incorporate networked bus[9] architectures susceptible to cybersecurity threats. These threats have the potential to affect the airworthiness of the airplane. These network architectures require cybersecurity provisions to address vulnerabilities to IUEI.[10] The FAA currently addresses transport category airplane security through the issuance of special conditions requiring proposed designs to isolate or protect vulnerable systems from unauthorized internal or external access.

Over time, the FAA has observed that repeated issuance of project-specific ASISP special conditions could result in cybersecurity-related certification criteria that are neither standardized between projects nor harmonized between the FAA and other Civil Aviation Authorities. These disconnects increase the certification complexity, cost, and

---

[8] The Report primarily recommended that the FAA undertake policy rather than regulatory changes to address cybersecurity on small airplanes and rotorcraft. *See, e.g.*, sections 2.3 and 2.4 of the Report.

[9] A bus is a communication system that transfers data between components inside a computer, or between computers.

[10] The FAA uses the term "security" in our rules rather than cybersecurity.

time for both the applicant and regulator. This proposed rulemaking package codifies the substantive requirements of frequently-issued cybersecurity special conditions to address these issues.

II. Authority for this Rulemaking

The FAA's authority to issue rules on aviation safety is found in title 49 of the United States Code. Subtitle I, section 106 describes the authority of the FAA Administrator. Subtitle VII, Aviation Programs, describes in more detail the scope of the agency's authority.

This rulemaking is issued under the authority described in subtitle VII, part A, subpart III, section 44701, "General Requirements." Under that section, the FAA is charged with prescribing regulations that promote safe flight of civil aircraft in air commerce by prescribing regulations and minimum standards for the design and performance of aircraft that the Administrator finds necessary for safety in air commerce. This regulation is within the scope of that authority as it prescribes new safety standards for the design and performance of transport category airplanes, engines, and propellers.

III. Discussion of the Proposed Rule

A. Protection of Transport Airplanes, Engines, and Propellers from IUEI

The FAA is proposing to add new §§ 25.1319, 33.28(n), 35.23(f), and revise their associated appendices, to protect against IUEI that may result in adverse effects on the safety of transport category airplanes, engines, and propellers. The proposed rule would implement ARAC recommendations, harmonize with the corresponding EASA CSs, and

reduce if not eliminate the need for the FAA to continue to issue project-specific special conditions addressing cybersecurity threats.

The proposed rule would require applicants to "protect" transport category airplanes, engines, and propellers from IUEI that may result in adverse effects on safety. To provide such protection for each product, applicants would be required by regulation to "identify and assess" the security risks posed by IUEI, and to "mitigate" those risks as necessary for safety, functionality, and continued airworthiness.

- For such identification and assessment of security risk, the applicant would be required to perform a security risk analysis to identify all threat conditions associated with the system, architecture, and external or internal interfaces.
- The FAA would expect such risk analysis to assess the severity of the effect of threat conditions on associated assets (system, architecture, etc.), consistent with the means of compliance the applicant has been using to meet the FAA's special conditions on this topic.
- Such assessment would also need to analyze these vulnerabilities for the likelihood of exploitation.
- The proposed regulation would then require each applicant to "mitigate" the vulnerabilities, and the FAA expects such mitigation would occur through the applicant's installation of single or multilayered protection mechanisms or process controls to ensure functional integrity, i.e., protection.

- Finally, each applicant would be required to include the procedures within their instructions for continued airworthiness necessary to maintain such protections.[11]
- Pursuant to 14 CFR 21.21(b), determinations regarding whether applicants have sufficiently identified and mitigated the security risks from IUEI would be made by the Administrator.

B. Transport Category Airplane Protection (Proposed 14 CFR 25.1319)

The requirements of proposed § 25.1319 are substantively based on the ASISP special conditions the FAA has issued in past transport airplane certification projects and the recommendations of the ARAC ASISP report. The FAA expects applicants would continue meeting the same objectives required by the ASISP special conditions and EASA's cybersecurity standards.

The FAA proposes that to adequately "mitigate the security risks as necessary for safety, functionality, and continued airworthiness" the applicant would generally need to show that the design accomplishes the first two requirements of the FAA's ASISP special conditions. First, that the design protects against unauthorized access from inside or outside of the airplane. Second, that the design prevents malicious changes to, and adverse impacts on, the airplane equipment, systems, and networks required for safe operation.

---

[11] Instructions for Continued Airworthiness contain the instructions and information necessary for the continued airworthiness of the aircraft, engine, propeller, parts, and appliances as required by the applicable Certification Basis.

In addition, certain proposed regulatory terms merit additional explanation. The term "IUEI" means a circumstance or event with the potential to affect the aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. Note that this definition includes malware and the effects of external systems on aircraft systems but does not include physical attacks or electromagnetic jamming. The new regulations would require applicants to consider the airplane's equipment, systems, and networks "separately and in relation to other systems." This language reflects the concern discussed in the ARAC ASISP report that cybersecurity threats can propagate from one system to another.[12]

The FAA also acknowledges that only IUEI vulnerabilities that may result in adverse effects on safety of the airplane require protection. This condition would limit the scope of the required protection to those effects that could impact the safety and airworthiness of the aircraft and its operation. For example, the ARAC ASISP report noted that, while devices used to process passenger credit cards may raise security issues related to passenger information, means other than airworthiness regulations would address such issues unless they also could impact systems with the potential to adversely affect the safety of the airplane.[13]

---

[12] Report, pp. 22, 152, and 182.

[13] Report, pp. 22 and 69.

The regulatory language used for the proposed §§ 25.1319, 33.28(n), 35.23(f), and their associated appendices build upon these concepts in the same manner. While EASA chose to adopt the ARAC's recommended wording directly, the FAA formatted the language to match existing FAA regulations.

C. Engine Control System and Propeller Control System Protections (Proposed 14 CFR 33.28 and 35.23)

Engine and propeller systems increasingly incorporate networked bus architectures susceptible to cybersecurity threats. These threats have the potential to affect the airworthiness of part 25 airplanes. These network architectures require cybersecurity provisions to address vulnerabilities from IUEI. Engine and propeller protections against IUEI threats are important because unmitigated cyberattacks can adversely affect the propulsion control functions needed for safe operation of the aircraft. Such attacks could also cause data corruption in crew displays and in health monitoring parameters used in operation and maintenance decisions.

To address this need and respond to the recommendations in the ARAC ASISP report, the FAA proposes to add new §§ 33.28(n) "Engine Control System" and 35.23(f) "Propeller Control System" sections to parts 33 and 35 of title 14 respectively. The proposed rule addresses any engine and propeller systems installed in airplanes, equipment, and networks that are susceptible to IUEI. These systems can include control functions that modulate propulsion output, propulsion controls, monitoring functions that track the health of the engine's systems, communication functions such as data buses and

networks, and auxiliary equipment such as fuel, lube, or pneumatic subsystems with embedded electronics.

Like the part 25 proposed rule, the proposed engine and propeller rules would require the applicant to protect against IUEI that could result in adverse effects on the safety of the airplane. This protection is accomplished by identifying and assessing all security risks caused by IUEI and then mitigating the security risks as necessary for safety, functionality, and continued airworthiness. The FAA expects that applicants would assess such risks using a risk analysis methodology that identifies all system and network vulnerabilities, a common industry practice used to address cybersecurity threats, and determine which vulnerabilities require mitigation for safe operation.

D. Instructions for Continued Airworthiness

Further, proposed revisions to appendix H to part 25 and to appendix A to both parts 33 and 35 would require applicants to prepare all procedures and ICA necessary to ensure continued protection against IEUI. The proposed changes to the appendices of parts 33 and 35 would require the applicant to furnish these procedures and ICA to the first owner of any transport airplane, engine, or propeller and make them available to subsequent operators per 14 CFR 21.50(b). Operators must follow these procedures and instructions to maintain aircraft, engine, and propellor security protections.

The FAA intends that the phrase “procedures and instructions for continued airworthiness” convey that maintenance procedures for security protections extend beyond typical ICA content. To accomplish these maintenance procedures, operators

develop an Aircraft Network Security Program[14] based on the applicant's security guidance to ensure conformance to type design and continued airworthiness.

The term "transfer" in the proposed regulation addresses the following activities. The lifecycle of airplanes, engines, and propellers involves data transfers between the onboard and offboard systems that collect and analyze data for health monitoring, trending, and maintenance decisions. These data transfer and software reprogramming activities can create operational vulnerabilities that require the implementation of safeguards to maintain airworthiness. The FAA proposes that these regulations will address such vulnerabilities.

E. Harmonization

EASA CS-25 prescribes the airworthiness standards corresponding to 14 CFR part 25 for products certified by the European Union. For aircraft certification in general, where part 25 and CS-25 differ, an applicant must meet both airworthiness standards if it desires to obtain both a U.S. type certificate and the validation of the type certificate by foreign authorities. Otherwise, the applicant must obtain exemptions, equivalent level of safety findings, special conditions, or the foreign authority's equivalent to those as necessary to meet one standard in lieu of the other. This proposal harmonizes the FAA's parts 25, 33, and 35 ASISP requirements with those of EASA, which would benefit manufacturers and modifiers by providing them a single set of requirements with which they must show compliance, thereby reducing the cost and complexity of certification

[14] See AC 119-1A, Operational Authorization of Aircraft Network Security Program.

and codifying a consistent level of safety. Unlike the FAA's proposal, EASA developed its equivalent regulatory text to address a broader range of products aligned with a European Union Horizontal cybersecurity requirement imposed across all industries. The proposed rule would eliminate the need to issue special conditions during the certification process in a manner harmonized with EASA requirements.

This proposed regulatory framework would establish a set of cybersecurity airworthiness standards for the certification and continued airworthiness of transport category airplanes, engines, and propellers. These standards align with the requirements of previously-issued ASISP special conditions, ARAC recommendations, and the corresponding EASA CS. As noted above, this framework would also have the benefit of reducing cost and time to certify new and changed products for both industry and the FAA.

F. Advisory Material for Proposed §§ 25.1319, 33.28, and 35.23 Miscellaneous Amendments

The FAA has developed proposed Advisory Circular (AC) 20-XXX, "Aircraft Systems Information Security/Protection (ASISP)." This AC would provide guidance on an acceptable means, but not the only means, of showing compliance with proposed §§ 25.1319, 33.28(n), and 35.23(f). It refers to the guidance materials that applicants have been using to show compliance with commonly issued special conditions. The FAA has placed this AC into the docket for comment.

IV. Regulatory Notices and Analyses

Federal agencies consider the impacts of regulatory actions under a variety of Executive orders and other requirements. First, Executive Order 12866 and Executive Order 13563, as amended by Executive Order 14094 ("Modernizing Regulatory Review"), direct that each Federal agency shall propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (Pub. L. 96-354) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (Pub. L. 96-39) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (Pub. L. 104-4) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate that may result in the expenditure by State, local, or Tribal governments, in the aggregate, or by the private sector, of $100 million or more (adjusted annually for inflation) in any one year. The current threshold after adjustment for inflation is $183 million using the most current (2023) Implicit Price Deflator for the Gross Domestic Product. This portion of the preamble presents the FAA's analysis of the economic impacts of this proposed rule.

In conducting these analyses, the FAA has determined that this proposed rule (1) would have benefits that justify its costs, (2) is not a "significant regulatory action" as defined in section 3(f) of Executive Order 12866, as amended; (3) would not have a significant economic impact on a substantial number of small entities; (4) would not create unnecessary obstacles to the foreign commerce of the United States; and (5) would

not impose an unfunded mandate on State, local, or Tribal governments, or on the private sector by exceeding the threshold identified above.

A. Regulatory Evaluation

The intended effects of this proposal would be to 1) incorporate the substance of the requirements contained in commonly issued ASISP special conditions, 2) reduce the cost and time necessary to certify new and changed products for both industry and the FAA; 3) harmonize FAA regulations with EASA cybersecurity CS; and 4) address ARAC recommendations. Subsequently, this proposal would create a cost savings for the FAA and the applicant by eliminating the need to continue issuing similar ASISP special conditions.

Aircraft, engines, and propellers increasingly incorporate networked bus architectures susceptible to cybersecurity threats. These threats have the potential to affect the airworthiness of the airplane. These network architectures require cybersecurity provisions to address vulnerabilities to IUEI.

The proposed rule may affect all five U.S. entities manufacturing transport category airplanes, four entities manufacturing engines for transport category airplanes, and four entities manufacturing propellers. Additionally, operators could have modifiers retrofit legacy airplanes with systems that would require cybersecurity provisions. The proposed changes to parts 25, 33, and 35 would apply to applicants for design approval of transport category airplanes, engines, and propellers. Under the proposed rule, the FAA would apply the requirements currently contained in the ASISP special conditions. This

action would reduce the costs and time to certify new and changed products while maintaining the level of safety provided by current ASISP special conditions.

Type certification of engines and propellers against cybersecurity threats has not required the issuance of special conditions. An issue paper provided to applicants describes an acceptable means of compliance for existing §§ 33.28, 33.75, 35.15, and 35.23 rules for these systems. The MoC contains FAA-accepted industry standards for protection against cybersecurity threats.[15] This proposal would codify the requirements for engine control systems and propeller control systems in §§ 33.28(n) and 35.23(f), respectively. Appendix A of these parts would contain the requirements for the applicant to develop procedures and ICA.

The FAA estimated the cost savings from eliminating ASISP special conditions over a ten-year period. The FAA assumes that, in absence of this proposed rule,[16] an equivalent number of special conditions processed from 2013 to 2022 would occur in the next ten years. The FAA processed and issued a total of 68 special conditions for cybersecurity from 2013 through 2022.

The FAA estimates, it would take about 170 hours of FAA's time to process a special condition application of average complexity. The FAA acknowledges that special conditions can vary in complexity. However, for purposes of this analysis, the FAA

---

[15] For example, cybersecurity standards that have been passed by RTCA and the European Organization for Civil Aviation Equipment (EUROCAE) are an FAA-accepted Means of Compliance.

[16] The FAA acknowledges that upon finalization of this proposed rule cybersecurity special conditions may still be required on occasion.

estimates its time savings from the elimination of ASISP special conditions to average about 170 hours. Multiplying the forecast for special conditions processed annually by processing time provides an estimate for the total time savings from the elimination of cybersecurity special conditions for the FAA over a ten-year period.

The process of issuing special conditions involves engineers, technical writers, and managers, and its cost averages $13,498 per special condition. To calculate the cost savings from reducing the number of special conditions, the FAA multiplied the forecast for the number of special conditions issued by its corresponding processing cost.

In summary, over a 10-year period of analysis, this proposal would result in a present value of cost savings for the FAA of about $783,366 at a three percent discount rate with an annualized cost savings of about $91,834. Applying a seven percent discount rate would result in a present value cost savings of about $645,584 with an annualized net cost savings of $91,916.

The cost savings above does not include the applicants for type certificates for transport category airplanes that would result from the elimination of the need to issue ASISP special conditions due to a lack of information. The FAA requests information for this group of applicants, along with supporting data, for the estimated time and cost savings.

B. Regulatory Flexibility Act

The Regulatory Flexibility Act (RFA) of 1980, (5 U.S.C. 601–612), as amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (Pub. L. 104–121) and the Small Business Jobs Act of 2010 (Pub. L. 111–240,), requires Federal agencies to

consider the effects of the regulatory action on small business and other small entities and to minimize any significant economic impact. The term "small entities" comprises small businesses and not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000.

The FAA is publishing this Initial Regulatory Flexibility Analysis (IRFA) to aid the public in commenting on the potential impacts on small entities from this proposal. The FAA invites interested parties to submit data and information regarding the potential economic impact that would result from the proposal. The FAA will consider comments when making a determination or when completing a Final Regulatory Flexibility Assessment.

An IRFA must contain the following:

(1) A description of the reasons why the action by the FAA is being considered;

(2) A succinct statement of the objective of, and legal basis for, the proposed rule;

(3) A description of, and where feasible, an estimate of the number of small entities to which the proposed rule would apply;

(4) A description of the projected reporting, recordkeeping, and other compliance requirements of the proposed rule, including an estimate of the classes of small entities that would be subject to the requirement and the type of professional skills necessary for the preparation of the report or record;

(5) An identification, to the extent practicable, of all relevant Federal rules that may duplicate, overlap, or conflict with the proposed rule; and

(6) A description of any significant alternatives to the proposed rule which accomplish the stated objectives of applicable statutes, and which minimize any significant economic impact of the proposed rule on small entities.

Currently, five entities in the United States manufacture transport category airplanes, four entities manufacture engines for transport category airplanes, and four entities manufacture propellers. The table below provides the North American Industrial Classification System (NAICS) codes for manufacturing aircraft, aircraft engines, and aircraft propellers, along with the size standard in terms of number of employees established by the Small Business Administration.[17]

Table 1

NAICS Code	Description	Size Standard
336411	Aircraft Manufacturing	1,500 employees
336412	Aircraft Engine and Engine Parts Manufacturing	1,500 employees
336413	Other Aircraft Parts and Auxiliary Equipment Manufacturing	1,250 employees

Based on the Small Business Administration (SBA) size standard for NAICS Code 336411 Aircraft Manufacturing, and NAICS Code 336412 Aircraft Engine and Engine Parts Manufacturing, the five transport category airplane manufacturers and four transport airplane engine manufacturers are not classified as small.

[17] Small Business Administration, Table of Small Business Size Standards Matched to NAICS Codes. Effective March 17, 2023. www.sba.gov/document/support--table-size-standards.

Of the four U.S. manufacturers of propellers (NAICS code 336413), only one had published data for their number of employees. The entity with published data is not categorized as small by SBA standards. The FAA does not know how many people the three remaining propeller manufacturers employ. Therefore, the FAA does not know whether these three remaining manufacturers are small entities.

This proposed rulemaking would standardize the FAA's criteria for addressing cybersecurity threats for transport category airplanes, engines, and propellers to reduce certification costs and time while maintaining the same level of safety provided by current special conditions. Therefore, it results in cost savings for the industry. The FAA welcomes comments on this analysis.

C. International Trade Impact Assessment

The Trade Agreements Act of 1979 (Pub. L. 96-39), as amended by the Uruguay Round Agreements Act (Pub. L. 103-465), prohibits Federal agencies from establishing standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. Pursuant to these Acts, the establishment of standards is not considered an unnecessary obstacle to the foreign commerce of the United States, so long as the standard has a legitimate domestic objective, such as the protection of safety, and does not operate in a manner that excludes imports that meet this objective. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards.

The FAA has assessed the potential effect of this proposed rule and determined that its objective is to promote the safety of the American public and does not exclude

imports that meet this objective. As a result, the FAA does not consider this proposed rule as creating an unnecessary obstacle to foreign commerce.

D. Unfunded Mandates Assessment

The Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531-1538) governs the issuance of Federal regulations that require unfunded mandates. An unfunded mandate is a regulation that requires a State, local, or Tribal government or the private sector to incur direct costs without the Federal Government having first provided the funds to pay those costs. The FAA determined that the proposed rule would not result in the expenditure of $183 million or more by State, local, or Tribal governments, in the aggregate, or the private sector, in any one year.

E. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (44 U.S.C. 3507(d)) requires that the FAA consider the impact of paperwork and other information collection burdens imposed on the public. The FAA has determined that there would be no new requirement for information collection associated with this proposed rule.

F. International Compatibility

In keeping with U.S. obligations under the Convention on International Civil Aviation, it is FAA policy to conform to International Civil Aviation Organization (ICAO) Standards and Recommended Practices to the maximum extent practicable. The FAA has reviewed the corresponding ICAO Standards and Recommended Practices and has identified no differences with these proposed regulations.

G. Environmental Analysis

FAA Order 1050.1F identifies FAA actions that are categorically excluded from the preparation of an environmental assessment or environmental impact statement under the National Environmental Policy Act (NEPA) in the absence of extraordinary circumstances. The FAA has determined this proposed rulemaking action qualifies for the categorical exclusion identified in paragraph 5-6.6f for regulations and involves no extraordinary circumstances.

V. Executive Order Determinations

A. Executive Order 13132, Federalism

The FAA has analyzed this proposed rule under the principles and criteria of Executive Order (E.O.) 13132, Federalism. The FAA has determined that this proposed action would not have a substantial direct effect on the States, the relationship between the Federal Government and the States, or the distribution of power and responsibilities among the various levels of government, and, therefore, would not have federalism implications.

B. Executive Order 13175, Consultation and Coordination with Indian Tribal Governments

Consistent with Executive Order 13175, Consultation and Coordination with Indian Tribal Governments,[18] and FAA Order 1210.20, American Indian and Alaska Native Tribal Consultation Policy and Procedures,[19] the FAA ensures that Federally

---

[18] 65 FR 67249 (November 6, 2000).

[19] See FAA Order No. 1210.20, dated January 28, 2004, https://www.faa.gov/documentLibrary/media/1210.pdf.

Recognized Tribes (Tribes) are given the opportunity to provide meaningful and timely input regarding proposed Federal actions that have the potential to affect uniquely or significantly their respective Tribes. At this point, the FAA has not identified any unique or significant effects, environmental or otherwise, on tribes resulting from this proposed rule.

C. Executive Order 13211, Regulations that Significantly Affect Energy Supply, Distribution, or Use

The FAA analyzed this proposed rule under E.O. 13211, Actions Concerning Regulations that Significantly Affect Energy Supply, Distribution, or Use (May 18, 2001). The FAA has determined that it would not be a "significant energy action" under the Executive order and would not be likely to have a significant adverse effect on the supply, distribution, or use of energy.

D. Executive Order 13609, Promoting International Regulatory Cooperation

Executive Order 13609, Promoting International Regulatory Cooperation, promotes international regulatory cooperation to meet shared challenges involving health, safety, labor, security, environmental, and other issues and reduce, eliminate, or prevent unnecessary differences in regulatory requirements. The FAA has analyzed this proposed action under the policy and agency responsibilities of E.O. 13609. The FAA has determined that this proposed action would eliminate differences between U.S. aviation standards and those of other civil aviation authorities.

VI. Additional Information

A. Comments Invited

The FAA invites interested persons to participate in this rulemaking by submitting written comments, data, or views. The FAA also invites comments relating to the economic, environmental, energy, or federalism impacts that might result from adopting the proposal in this document. The most helpful comments reference a specific portion of the proposal, explain the reason for any recommended change, and include supporting data. To ensure the docket does not contain duplicate comments, commenters should submit only one time if comments are filed electronically, or commenters should send only one copy of written comments if comments are filed in writing.

The FAA will file in the docket all comments it receives, as well as a report summarizing each substantive public contact with FAA personnel concerning this proposed rulemaking. Before acting on this proposal, the FAA will consider all comments it receives on or before the closing date for comments. The FAA will consider comments filed after the comment period has closed if it is possible to do so without incurring expense or delay. The FAA may change this proposal in light of the comments it receives.

B. Confidential Business Information

Confidential Business Information (CBI) is commercial or financial information that is both customarily and actually treated as private by its owner. Under the Freedom of Information Act (FOIA) (5 U.S.C. 552), CBI is exempt from public disclosure. If your comments responsive to this NPRM contain commercial or financial information that is customarily treated as private, that you actually treat as private, and that is relevant or responsive to this NPRM, it is important that you clearly designate the submitted

comments as CBI. Please mark each page of your submission containing CBI as "PROPIN." The FAA will treat such marked submissions as confidential under the FOIA, and they will not be placed in the public docket of this NPRM. Submissions containing CBI should be sent to the person in the **FOR FURTHER INFORMATION CONTACT** section of this document. Any commentary that the FAA receives that is not specifically designated as CBI will be placed in the public docket for this rulemaking.

C. Electronic Access and Filing

A copy of this NPRM, all comments received, any final rule, and all background material may be viewed online at www.regulations.gov using the docket number listed above. A copy of this proposed rule will be placed in the docket. Electronic retrieval help and guidelines are available on the website. It is available 24 hours a day, 365 days a year. An electronic copy of this document may also be downloaded from the Office of the Federal Register's website at www.federalregister.gov and the Government Publishing Office's website at www.govinfo.gov. A copy may also be found at the FAA's Regulations and Policies website at www.faa.gov/regulations_policies.

Copies may also be obtained by sending a request to the Federal Aviation Administration, Office of Rulemaking, ARM-1, 800 Independence Avenue SW, Washington, DC 20591, or by calling (202) 267-9677. Commenters must identify the docket or notice number of this rulemaking.

All documents the FAA considered in developing this proposed rule, including economic analyses and technical reports, may be accessed in the electronic docket for this rulemaking.

D. Small Business Regulatory Enforcement Fairness Act

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires the FAA to comply with small entity requests for information or advice about compliance with statutes and regulations within its jurisdiction. A small entity with questions regarding this document may contact its local FAA official, or the person listed under the **FOR FURTHER INFORMATION CONTACT** section of this document. To find out more about SBREFA on the Internet, visit www.faa.gov/regulations_policies/rulemaking/sbre_act/.

List of Subjects

14 CFR Part 25

Aircraft, Aviation safety, Navigation (air), Reporting and recordkeeping requirements.

14 CFR Part 33

Aircraft, Aviation safety, Reporting and recordkeeping requirements.

14 CFR Part 35

Aircraft, Aviation safety.

The Proposed Amendment

In consideration of the foregoing, the Federal Aviation Administration proposes to amend chapter I of title 14, Code of Federal Regulations as follows:

PART 25—AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES

1. The authority citation for part 25 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g), 40113, 44701, 44702 and 44704; Pub. L. 115-254, 132 Stat 3281 (49 U.S.C. 44903 note).

2. Add § 25.1319 under the undesignated center heading "General" to read as follows:

§ 25.1319 Equipment, systems, and network information security protection.

(a) *Airplane equipment, systems, and network information security protection.* Airplane equipment, systems, and networks—considered separately and in relation to other systems—must be protected from intentional unauthorized electronic interactions that may result in adverse effects on the safety of the airplane. The applicant must—

(1) Identify and assess the security risks from all intentional unauthorized electronic interactions.

(2) Mitigate the security risks as necessary for safety, functionality, and continued airworthiness.

(3) Prepare and make available all procedures and instructions for continued airworthiness necessary to maintain security protections in accordance with appendix H to this part.

(b) [Reserved]

3. In appendix H:

a. Under the heading H25.1, revise paragraph (a); and

b. Under the heading H25.3, add paragraph (h);

The revision and addition read as follows:

Appendix H to Part 25—Instructions for Continued Airworthiness

H25.1 *General*.

(a) This appendix specifies requirements for preparation of Instructions for Continued Airworthiness as required by §§ 25.1319, 25.1529, 25.1729, and applicable provisions of parts 21 and 26 of this chapter.

* * * * *

H25.3 *Content*.

* * * * *

(h) Procedures and instructions necessary to maintain airplane security protections from intentional unauthorized electronic interactions.

* * * * *

PART 33—AIRWORTHINESS STANDARDS: AIRCRAFT ENGINES

5. The authority citation for part 33 continues to read as follows:

Authority: 49 U.S.C. 106(g), 40113, 44701, 44702, 44704.

6. In § 33.28, add paragraph (n) to read as follows:

§ 33.28 Engine control systems.

* * * * *

(n) *Engine equipment, systems, and network information security protection.* Engine control, monitoring and auxiliary equipment, systems, and networks—considered separately and in relation to other systems—must be protected from intentional

unauthorized electronic interactions that may result in adverse effects on the safety of the engine or the aircraft. The applicant must—

(1) Identify and assess the security risks from all intentional unauthorized electronic interactions.

(2) Mitigate such security risks as necessary for safety, functionality, and continued airworthiness.

(3) Prepare and make available all procedures and instructions for continued airworthiness necessary to maintain security protections in accordance with appendix A to this part.

7. In appendix A, under the heading a33.3, add paragraph (a)(10) to read as follows:

Appendix A to Part 33—Instructions for Continued Airworthiness

* * * * *

a33.3 content

* * * * *

(a) * * *

(10) Procedures and instructions for transfer of engine control software, monitoring software, and data between aircraft, engines, and ground systems to maintain information security protections as required by § 33.28(n).

* * * * *

PART 35—AIRWORTHINESS STANDARDS: PROPELLERS

8. The authority citation for part 35 continues to read as follows:

Authority: 49 U.S.C. 106(f), 106(g), 40113, 44701-44702, 44704.

9. In § 35.23, add paragraph (f) to read as follows:

§ 35.23 Propeller control system.

* * * * *

(f) Propeller control, monitoring and auxiliary equipment, systems, and networks—considered separately and in relation to other systems—must be protected from intentional unauthorized electronic interactions that may result in adverse effects on the safety of the propeller or the aircraft. The applicant must—

(1) Identify and assess the security risks from all intentional unauthorized electronic interactions.

(2) Mitigate such security risks as necessary for safety, functionality, and continued airworthiness.

(3) Prepare and make available all procedures and instructions for continued airworthiness necessary to maintain security protections in accordance with appendix A to this part.

10. In appendix A, under the heading a35.3, add paragraph (a)(10) to read as follows:

Appendix A to Part 35—Instructions for Continued Airworthiness

* * * * *

a35.3 content

(a) * * *

(10) Procedures and instructions for transfer of propeller control software, monitoring software, and data between aircraft, propellers, and ground systems to maintain information security protections as required by § 35.23(f).

* * * * *

Issued under authority provided by 49 U.S.C. 106(f) and 44701(a), and 44703 in Washington, DC.

Wesley L. Mooty,

Acting Executive Director, Aircraft Certification Service.

[FR Doc. 2024-17916 Filed: 8/20/2024 8:45 am; Publication Date: 8/21/2024]