NOTICE

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

National Policy

N 8110.118

Effective Date:
MM/DD/YYYY

Cancellation Date:
MM/DD/YYYY

SUBJ: Submittal and Disclosure of Safety Critical Information by Applicants for Transport Category Airplane Type Certificates

1. Purpose of This Notice. This Notice supplements Federal Aviation Administration (FAA) Order 8110.4C, Type Certification, and explains FAA interim policy regarding some of the requirements of Section 105(a) of The Aircraft Certification, Safety, and Accountability Act, Pub. L. 116-260 (the Act). Section 105(a) of the Act established paragraph 44704(e) of Title 49, United States Code (49 U.S.C.). The Act mandates that the Administrator require the submittal and disclosure of safety critical information by applicants for, or holders of, new or amended, but not supplemental, type certificates (TC) for transport category airplanes covered under title 14, Code of Federal Regulations part 25. Section 105(a) also mandates the FAA to establish multiple milestones throughout the certification process at which a proposed airplane system will be assessed to determine whether any change to such system during the certification process is such that the system should be considered novel or unusual by the Administrator.

The FAA is initiating rulemaking that will propose to mandate, after notice and an opportunity for the public to comment, Section 105(a)'s requirements for transport category airplane new and amended TC applicants and holders. However, this Notice addresses methods of clearly identifying, as "safety critical", certain information that already is, and can continue to be, provided by applicants during the application process for a new or amended TC project for a transport category airplane. The Notice also discusses usage of milestones throughout the project.

2. Audience. The audience for this Notice is TC applicants, Aircraft Certification Service personnel, Flight Standards Service personnel, Aircraft Evaluation Division personnel, and FAA individual and organizational designees.

3. Where Can I Find This Notice? You can find this Notice on the internet at http://www.faa.gov/regulations_policies/orders_notices/.

4. Background.

a. New Statutory Requirement. Section 105(a), Disclosure, amended Section 44704 of Title 49, United States Code (49 U.S.C.). New section 49 USC 44704(e)(1)-(2) provides the following direction to the FAA:

(e) DISCLOSURE OF SAFETY CRITICAL INFORMATION. —

(1) IN GENERAL.—Notwithstanding a delegation described in section 44702(d), the Administrator shall require an applicant for, or holder of, a type certificate for a transport category airplane covered under part 25 of title 14, Code of Federal Regulations, to submit safety critical information with respect to such airplane to the Administrator in such form, manner, or time as the Administrator may require. Such safety critical information shall include —

(A) any design and operational details, intended functions, and failure modes of any system that, without being commanded by the flightcrew, commands the operation of any safety critical function or feature required for control of an airplane during flight or that otherwise changes the flight path or airspeed of an airplane;

(B) the design and operational details, intended functions, failure modes, and mode annunciations of autopilot and autothrottle systems, if applicable;

(C) any failure or operating condition that the applicant or holder anticipates or has concluded would result in an outcome with a severity level of hazardous or catastrophic, as defined in the appropriate Administration airworthiness requirements and guidance applicable to transport category airplanes defining risk severity;

(D) any adverse handling quality that fails to meet the requirements of applicable regulations without the addition of a software system to augment the flight controls of the airplane to produce compliant handling qualities; and

(E) a system safety assessment with respect to a system described in subparagraph (A) or (B) or with respect to any component or other system for which failure or erroneous operation of such component or system could result in an outcome with a severity level of hazardous or catastrophic, as defined in the appropriate airworthiness requirements and guidance applicable to transport category airplanes defining risk severity.

(2) ONGOING COMMUNICATIONS.—

(A) NEWLY DISCOVERED INFORMATION.—The Administrator shall require that an applicant for, or holder of, a type certificate disclose to the Administrator, in such form, manner, or time as the Administrator may require, any newly discovered information or design or analysis change that would materially alter any submission to the Administrator under paragraph (1).

(B) SYSTEM DEVELOPMENT CHANGES.—The Administrator shall establish multiple milestones throughout the certification process at which a proposed airplane system will be assessed to determine whether any change to such system during the certification process is such that such system should be considered novel or unusual by the Administrator.

* * * * *

(7) DEFINITION OF TYPE CERTIFICATE.—In this subsection, the term 'type certificate'—

(A) means a type certificate issued under subsection (a) or an amendment to such certificate; and
(B) does not include a supplemental type certificate issued under subsection (b).

b. Current Submittal and Review Processes Relevant to Section 105(a) - Applicant Submittals. 14 CFR § 21.15 requires applications for TCs to be made on a form and in a manner prescribed by the FAA. Section 21.15(b) requires the application to be accompanied by "available preliminary basic data." Section 21.20 requires the applicant to show compliance with all applicable requirements, provide the FAA the means by which such compliance has been shown, and certify that the applicant has complied. For a transport category airplane, the applicant must show compliance with the substantive design regulations of part 25, including 14 CFR §§ 25.1301 and 25.1309. Per 14 CFR § 21.21(b), the FAA examines this information, including the proposed type design, in order to find compliance. The applicant's showings, and the FAA's findings of compliance, are part of the approved TC.

To ensure that such required showings and findings can be timely[1] and accurately made, applicants and the FAA may negotiate a plan. With submittal of the required application, applicants may submit a proposed certification plan[2] as a mechanism for communicating key project information to the FAA. In accordance with paragraph 2-3d of FAA Order 8110.4C, the plan may provide information on the applicant's proposed design, and on how the applicant plans to show that it complies with FAA regulations. The plan may include a proposed project schedule with milestones.

(1) Applicant Showings of Compliance. FAA Order 8110.4C, paragraph 2-6k, states that compliance data should be submitted as soon as complete, so that FAA's review can be accomplished during the normal course of a certification project.

The proposed certification plan should include the proposed certification basis (including a compliance checklist). Per current policy and practice, the information provided in the proposed certification plan should be sufficiently developed, and detailed, to enable the FAA to determine its level of involvement for each compliance showing and finding, facilitate the collection of all necessary compliance data, and to allow all showings and findings[3] to be timely and accurately made for each project.

(2) Milestones. FAA Order 8110.4C also provides for the applicant and FAA to establish agreed-upon milestones to facilitate the timely submission and review of information during the

[1] 14 CFR § 21.17(c) limits the duration of type certificate applications.
[2] *The FAA and Industry Guide to Product Certification*, (3rd Ed., March 2017), differs from FAA Order 8110.4C, in that it describes, at section 3.1, the applicant's proposed plan as the "Project Specific Certification Plan."
[3] FAA Order 8110.4C, paragraphs 2-3d(1) through (11) and 2-5(d).

type certification process. Paragraph 2-3d(9) recommends the provision of information on the applicant's proposed schedule including milestones, such as preliminary hazard analysis submittal dates, substantiating data submittal dates, conformity and testing completion dates, and expected date of final certification.

(3) Type Certificate. 14 CFR § 21.41 defines the TC, which includes the type design, the operating limitations, the type certificate data sheet (TCDS), the applicable regulations of 14 CFR, Chapter I, subchapter C, with which the FAA records compliance, and any other conditions or limitations prescribed for the product in this subchapter. Paragraph 3-3 of Order 8110.4C recommends additional information to document the conditions and limitations necessary to meet certification airworthiness requirements and the information to be listed on the TCDS.

5. Policy. This Notice provides guidance on how to use the aforementioned certification plan as a conduit for the applicant's submittal of safety critical information, for transport category airplanes covered under part 25. It also provides guidance for this information to be regularly updated, per Section 105(a), at milestones defined within the agreed-upon project-specific certification plan.

Furthermore, this Notice recommends processes for the FAA to receive and review the safety critical information defined by Section 105(a). These recommended processes will ensure that the design and operational details associated with airplane systems, or any change to them during the certification process, are adequately identified and disclosed by the applicant. Also, these recommended processes will supplement the FAA's current processes for determining whether any change to such system during the certification process is such that the system should be considered novel or unusual (reference 14 CFR §§ 21.16 and 21.101(d)) by the Administrator.

The processes discussed in this Notice apply only to transport category airplane TC and amended TC projects as described by the Act.

a. Submittal of Safety Critical Information with Proposed Certification Plan. The FAA is initiating rulemaking to implement the Section 105(a) requirement that the Administrator require an applicant for a new or amended TC, but not a supplemental TC, submit safety critical information in such form, manner, or time as required by the Administrator. However, safety critical information is already provided to the FAA pursuant to existing aforementioned certification regulations and processes, though such information may not be currently identified by applicants as "safety critical." As noted above, an applicant for a new TC or amended TC for a transport category airplane may currently provide a proposed certification plan, with certain planning information, when submitting an application. Thus, this proposed certification plan should delineate, as discussed below, the project's safety critical information (as defined by U.S.C. 44704(e)).[4] The information, including the level of detail, provided by the initial proposed certification plan should be sufficient to allow the FAA to identify the applicant's

[4] See Appendix 1, Safety Critical Information Matrix, for information on mapping certain part 25 airworthiness requirements, for which showings of compliance must be made, with the categories of safety critical information that must be disclosed.

deliverables and provide clarity for how the applicant plans to comply with the applicable regulations. This will facilitate the FAA's processing of the application.

The type design for a transport category airplane project will likely not be sufficiently developed at the time of project application to enable the inclusion of all safety critical information within the proposed certification plan. However, applicants should delineate safety critical information and anticipated deliverables within the compliance checklist and preliminary system safety assessment sections and referenced documentation. This initial proposed certification plan may be based on preliminary designs and concepts, and will necessitate subsequent updates as the applicant's proposed type design is refined through tests, analyses, and inspections. As discussed below, these planned updates should be included as milestones within the initial proposed certification plan to establish "gates" throughout the certification process at which a proposed airplane's systems, design and operational details, and associated documentation will be presented and assessed for changes and impacts to the overall certification approach (e.g., certification basis, traceability, compliance dependencies, means of compliance, etc.) for the project.

Note: An applicant may be uncertain if a particular design or analysis change will be part of its final design, and the FAA is not suggesting that applicants provide the FAA with design changes that are still speculative. However, applicants should inform the FAA when it becomes more likely than not that the design or analysis change will be incorporated or information previously submitted is no longer valid, appropriate, or sufficient.

b. Establishing Milestones and Updating Safety Critical Information During the Certification Process (Newly Discovered Information). Per Section 105(a), the Administrator must require applicants for TCs to disclose to the Administrator, in such form, manner, or time as the Administrator may require, any newly discovered information or design or analysis change that would materially alter[5] any submission of safety critical information. As discussed above, the FAA is developing rulemaking to implement Section 105(a)'s requirements. However, in order to allow the required showings and findings of compliance to be timely and accurately made, the applicant should already keep this information current throughout the certification process, and expeditiously disclose to the FAA any new information or proposed design or analysis changes that would materially alter any prior submission of safety critical information.

FAA Order 8110.4C, paragraph 2-3d(9) is an existing recommended certification process that supports the need for the Administrator to establish multiple milestones throughout the certification process, at which a proposed airplane system can be assessed to determine whether any change to that system is such that the system should be considered novel or unusual. Under this existing process, applicants may include a proposed project schedule within their certification plan. In addition to the typical milestones (such as for testing and submittals for descriptive and substantiating data) that the applicant and FAA use to plan the project, the proposed and approved schedule may already, and continue to, include sufficient milestones to

[5] "Materially alter" means potentially affecting or negating a compliance showing, impacting a certification assumption (e.g., design, human factors, operational training, etc.), or that would affect, the FAA's level of involvement (e.g., delegation decisions).

ensure the project's timely progress. These milestones include dates for submitting preliminary hazard analyses, system safety assessments (SSAs), fault tree analyses (FTAs), the requirements validation plan, software development documents, minimum training requirements[6] and other data to support the flight standardization board report and revisions (as needed), and functional hazard assessments (FHAs). During these recommended milestone reviews, the proposed airplane systems will be assessed jointly by the FAA and the applicant (e.g., through use of a system development and review process).

Updating Applicant System Safety Assessments. The safety assessment process is often used by applicants to show compliance with certain regulatory design standards that are relevant to the Section 105 categories of safety critical information, such as 14 CFR § 25.1309.[7] A common and FAA-accepted means of compliance with that regulation is SAE Aerospace Recommended Practice (ARP)4754A, *Guidelines for Development of Civil Aircraft and Systems*.[8] That document states that "the process includes specific assessments conducted and updated during system development and includes how it interacts with the other system development processes. The primary safety assessment processes are detailed in ARP4761…" and include safety assessment techniques such as the functional hazard assessment, preliminary aircraft safety assessment / preliminary system safety assessment, aircraft safety assessment / system safety assessment, and common cause analysis. Draft Advisory Circular (AC) 25.1309-1A, *System Design and Analysis* (the "Arsenal" version of such guidance), has a means of compliance, which, in conjunction with an equivalent level of safety finding, the FAA has accepted since 2001. This AC provides guidance on conducting planning activities and the functional and physical interrelationships of systems; determination of the details of means of compliance, means for validating accomplishment of the plan, and validation and verification.

The safety assessment techniques in SAE ARP4761, AC 25.1309-1A, and the "Arsenal" version of AC 25.1309-1A are iterative processes associated with the type design definition, and are conducted at multiple milestones[9] during system development. As such, applicants choosing to use those methods of compliance continually disclose changes to designs or analysis throughout the certification process, resulting in submittal of type design, test reports, and computations in accordance with 14 CFR § 21.20(b) as documented by the TC.

c. Issuance of the Type Certificate. Applicants are entitled to a TC after they show compliance, the FAA finds compliance, and the FAA finds that the type design has no unsafe features. It is the FAA who determines whether the applicant has shown compliance. Safety critical information, as defined by Section 105, is already included in type design, operating limitations, substantiating documentation and other required information, and is part of the TC. Thus, applicants choosing to utilize the certification planning processes of FAA Order 8110.4C

[6] 14 CFR 121, subpart N defines operator training programs.
[7] The FAA has proposed to revise 14 CFR § 25.1309, and AC 25.1309-1A, and may update this policy, if needed.
[8] SAE ARP4754A is an industry-recommended practice for the planning and execution of development assurance for commercial aircraft accepted by the FAA as a method of compliance per Advisory Circular (AC) 20-174, *Development of Civil Aircraft and Systems*.
[9] See SAE ARP4761, Appendix D for additional details on typical FTA timeline and milestones and ARP4754, Sections 1.0, 5.1.5, and 5.4.2 for principles of the safety assessment tasks, management and the schedule for deliverable items according to the milestones (reviews) of the development plan.

and supplemented by this Notice are able to submit and update this information, including safety critical information, required by14 CFR §§ 21.20 and 21.21(b).

6. Effect of Policy. The contents of this document, by itself, do not have the force and effect of law and are not meant to bind the public in any way. This document is intended only to provide information to the public regarding existing requirements under the law (including Section 105(a) and 14 CFR §§ 21.20 and 21.21) or agency policies.

7. Deviations. Any deviation to this Notice must be approved by AIR-600.

APPENDIX 1 – SAFETY CRITICAL INFORMATION MATRIX

This matrix maps certain airworthiness requirements (design standards) to the safety critical information as defined by 49 USC 44704(e). This matrix is not an inclusive list; it is the responsibility of the applicant to ensure their certification plan contains the necessary information to reflect their proposed certification project.

The shaded areas in Table 1 provide a correlation between specific airworthiness requirements and safety critical information categories to assist with including or describing safety critical information within a proposed certification plan. See each of the notes for additional information.

Table 1

Safety Critical Information	**§ 25.143(a)(b) - General.**	**§ 25.672 - Stability augmentation and automatic and power-operated systems.**	**§ 25.1301(a) Function and installation.**	**§ 25.1309(a) Equipment, systems, and installations.**	**§ 25.1309(b) Equipment, systems, and installations.**	**§ 25.1309(c) Equipment, systems, and installations.**	**§ 25.1309(d) Equipment, systems, and installations.**	**§ 25.1322 Flight crew alerting.**	**§ 25.1329 Flight guidance system (b)(c)(d)(e)(g)(h)(i)(j)(k)(l)(m)**
(A) any design and operational details, intended functions, and failure modes of any system that, without being commanded by the flightcrew, commands the operation of any safety critical function or feature required for control of an airplane during flight or that otherwise changes the flight path or airspeed of an airplane * See NOTE 1 below			X	X		X	X	X	X
(B) the design and operational details, intended functions, failure modes, and mode annunciations of autopilot and autothrottle systems, if applicable * See NOTE 2 below			X	X		X	X	X	X

(C) any failure or operating condition that the applicant or holder anticipates or has concluded would result in an outcome with a severity level of hazardous or catastrophic, as defined in the appropriate Administration airworthiness requirements and guidance applicable to transport category airplanes defining risk severity * See Note 3 below					X				
(D) any adverse handling quality that fails to meet the requirements of applicable regulations without the addition of a software system to augment the flight controls of the airplane to produce compliant handling qualities * See Note 4 below	X	X					X		
(E) a system safety assessment with respect to a system described in subparagraph (A) or (B) or with respect to any component or other system for which failure or erroneous operation of such component or system could result in an outcome with a severity level of hazardous or catastrophic, as defined in the appropriate airworthiness requirements and guidance applicable to transport category airplanes defining risk severity * See Note 5 below					X		X		

Note 1:

Applicable "systems." Systems which the FAA expects would be included within this category of safety critical information include flight control systems and other computer (software) controlled systems (e.g., autopilot, stability augmentation, flight guidance systems, autothrottle (autothrust), and control mode envelope protection), whose failure or erroneous activation would present a risk rated hazardous or catastrophic.

"Safety critical function or feature." For purposes of inclusion in this category of safety critical information, a "safety critical function or feature" is one whose failure would be hazardous or catastrophic.

"All design and operational details." Such "details" would be the ones of relevance to the system's function, failure, or operational suitability.

In order to show compliance with 14 CFR §§ 25.1301(a) and 25.1309(a), the compliance data must include sufficient design and operational detail and description of intended function that the FAA can assess whether the equipment is of a kind and design appropriate to its intended function and performs its intended function under any foreseeable operating condition.

Section 25.1309(d) requires the applicant submit an analysis of the possible modes of failure, probability of failures, resulting effects, etc. (i.e., a system safety assessment) to show compliance to 14 CFR § 25.1309(b).

Note 2:

"Autopilot" would be any aircraft system and associated sensors designed to provide automatic control of the pitch, roll, and in certain instances, yaw axis of an aircraft. This would include traditional autopilot function (to fly along a desired flight path) and also stability augmentation systems that can operate independently of the autopilot and make inputs to flight control surfaces.

"Autothrottle" would be any system selected by the crew to provide automatic engine thrust control, as required, to achieve and maintain desired aircraft speed or vertical flight profile.

A "mode annunciation" provides the flightcrew with awareness of the current automation mode, alerts them of any mode changes or failures that could degrade the handling or operational characteristics of the airplane and may require the pilot to alter their primary control strategy. The mode annunciation is included because it is imperative that the flightcrew understand the state of the airplane systems so they can interact with airplane systems appropriately as they fly the airplane.

The flight guidance system (as a piece of installed equipment) is subject to the 14 CFR §§ 25.1301 and 25.1309 sections discussed in this table, and, in addition, to the specific requirements of 14 CFR § 25.1329. Section 25.1329 covers the effects of mode switching, disengagement, failure to disengage, malfunctions, annunciations, etc.

In addition, 14 CFR §§ 25.1309(c) and 25.1322(a) flightcrew alerting requirements apply. Compliance data includes complete design details, system safety assessments, alerting assessment, human factors assessments, etc.

Note 3:

Section 25.1309(b) provides the required safety level for failure conditions. Section 25.1309(b)(1) corresponds to the "catastrophic" severity level except it does not prohibit single failures leading to catastrophic conditions.

Current approved FAA guidance for applicants addresses catastrophic failure and operating conditions, but does not explicitly address "hazardous" conditions; however, as previously discussed, the ARAC-recommended, and oft-used, "Arsenal" version of AC 25.1309-1A does so, and therefore modern applicants typically address hazardous failure and operating conditions in their SSAs.

"Hazardous" for purposes of this policy would be the following:

A failure condition that would reduce the capability of the airplane or the ability of the flightcrew to cope with adverse operating conditions to the extent that there would be -

- A large reduction in safety margins or functional capabilities,
- Physical distress or excessive workload such that the flightcrew cannot be relied upon to perform their tasks accurately or completely, or
- Serious or fatal injuries to a relatively small number of persons other than the flightcrew.[10]

"Catastrophic" for purposes of this rule would be a failure condition that would result in multiple fatalities, usually with the loss of the airplane.

[10] For the purpose of performing a safety assessment, a "small number" of fatal injuries means one such injury.

Note 4:

An “adverse” handling quality is one that does not meet the applicable handling qualities regulations in Subpart B of part 25. The “applicable regulations” for purposes of this category would be those in Subpart B of part 25. That subpart includes requirements for ensuring the airplane is aerodynamically stable, and predictable in its handling.

Software systems that augment flight controls (as a piece of installed equipment) are subject to the portions of 14 CFR §§ 25.1301 and 25.1309 discussed in Table 1, and, in addition, the specific requirements of 14 CFR § 25.672. Section 25.672 covers specific failure effects, alerting, controllability and maneuverability, etc. for such systems.

The handling qualities requirements are found in 14 CFR §§ 25.143(a) (safely controllable and maneuverable during...) and 25.143(b) (it must be possible to make a smooth transition from one flight condition to any other flight condition without exceptional piloting skill, alertness, or strength…).

Compliance data for these regulations includes complete design details, SSAs, alerting assessment, human factors assessments, handling qualities assessments etc.

The “flight characteristics requirements” of 14 CFR § 25.672 are found in part 25 subpart B.

Note 5:

Designs that have a system described in A or B will have this information in their SSAs, and everything from a “major” to a “hazardous” failure condition should be included.

Section 25.1309(d) requires the applicant submit an analysis of the possible modes of failure, probability of failures, resulting effects, etc. (i.e., an SSA) to show compliance to 14 CFR § 25.1309(b). The “Arsenal” version of AC 25.1309-1A provides additional guidance.