U.S. Department
of Transportation
Federal Aviation
Administration

Advisory Circular

Subject: Operational Authorization of Aircraft Network Security Program

Date: 9/28/23
Initiated by: AFS-300

AC No: 119-1A
Change:

1 **PURPOSE OF THIS ADVISORY CIRCULAR (AC).** This AC describes an acceptable means, but not the only means, of obtaining operational authorization for an aircraft certificated with a special condition (SC) related to the security of the onboard computer network. The current edition of RTCA DO-355, Information Security Guidance for Continuing Airworthiness, is an acceptable alternative to the information in this AC. However, the process to gain operations specification (OpSpec) authorization still resides in this AC.

1.1 This AC does not cover the physical security of the aircraft or the surrounding area. Existing Federal Aviation Administration (FAA) and Transportation Security Administration (TSA) regulations address compliance with physical security guidelines.

1.2 The contents of this document do not have the force and effect of law and are not meant to bind the public in any way, and the document is intended only to provide information to the public regarding existing requirements under the law or agency policies.

2 **AUDIENCE.** This AC is intended to be used by Title 14 of the Code of Federal Regulations (14 CFR) parts 121, 121/135, 125, and 129 operators during the initial authorization and lifespan of the FAA-authorized Aircraft Network Security Program (ANSP). The secondary audience includes all General Aviation and Air Carrier Safety Assurance offices with certificate oversight of operators conducting operations with aircraft requiring an ANSP.

Note: Where applicable, other operations may still be required to follow the design approval holder's (DAH) instructions related to electronic system security isolation or protection created to meet an SC.

3 **WHERE YOU CAN FIND THIS AC.** You can find this AC on the FAA's website at https://www.faa.gov/regulations_policies/advisory_circulars and the Dynamic Regulatory System (DRS) at https://drs.faa.gov.

4 **WHAT THIS AC CANCELS.** AC 119-1, Operational Authorization of Aircraft Network Security Program (ANSP), dated September 30, 2015, is canceled.

5 **WHY THE NEED FOR AN ANSP?** Previous aircraft designs utilized ARINC Specification 429, ARINC Specification 629, or Military Standard (MIL-STD) databuses to connect flight-critical avionics systems. Current designs have adopted several technological advances that create a potential for unauthorized persons to access the

aircraft control domain, and present security vulnerabilities related to the introduction of computer viruses and worms, user errors, and intentional sabotage of airplane electronic assets (e.g., networks, systems, and databases) critical to the safety and maintenance of the airplane. This advanced technology can be found not only in new aircraft designs but also in postdelivery modifications. SCs are issued to the DAH to ensure the security of the computer network. An operator, pursuant to 14 CFR part 119, needs authorization to operate aircraft that have been issued these SCs. This authorization to operate comes through an OpSpec. An ANSP based on the DAH's security documents is part of the OpSpec that ensures conformance to type design and continued airworthiness. Refer to part 119, § 119.49(a).

5.1 **Advanced Connectivity Technology Benefits.** A major benefit of advanced connectivity is the ability to move data to and from the aircraft without the use of standard storage media. The types of data transmitted can range from customer profile, In-Flight Entertainment (IFE) content, navigation, and aircraft health monitoring.

5.2 **Potential Data Security Risks.** As with other advanced connectivity, a real threat exists, that may be intentional or unintentional, with a detrimental effect on system performance. These effects may range from reduced performance to denial of service, due to accident or criminal activity.

5.3 **Data Security.** The transmission of critical data affecting airworthiness to and from the aircraft necessitates the need for an ANSP under the OpSpec. A comprehensive ANSP mitigates risk to network security on board the aircraft, the off-airport supporting infrastructure (e.g., corporate offices), and everything in between (including wired and wireless connectivity).

6 HOW DO I KNOW IF AN AIRCRAFT OPERATION NEEDS AN ANSP?

An aircraft requiring an ANSP under the OpSpec to operate is identified by an SC listed on the Type Certificate Data Sheet (TCDS), or, if later modified, an SC that will be identified in the Supplemental Type Certificate (STC) or amended type certificate (TC). In any of these cases, only SCs requiring instructions to an operator would trigger the need for an ANSP (see Appendix A, ANSP Applicability Decision Making Flowchart).

7 WHAT DOCUMENTS ARE USED TO CREATE AN ANSP?

7.1 **Special Condition (SC).** An SC is a rulemaking action that is specific to an aircraft's design and concerns a novel or unusual design feature that the Code of Federal Regulations (CFR) does not adequately or appropriately address. SCs are an integral part of the certification basis and give the manufacturer permission to build the aircraft, engine, or propeller with additional capabilities not referred to in the regulations. During the aircraft type certification process, it is the responsibility of the DAH to identify communication systems designed with connectivity external and internal to critical systems. The FAA's Aircraft Certification Service (AIR) will review and issue an SC that will be added to the TCDS (refer to 14 CFR part 21, § 21.16).

7.2 DAH Document. The DAH will submit aircraft network security guidance for operators to the responsible Aircraft Certification Service office for approval when showing compliance with an applicable SC. The network security guidance provides operators with information necessary to maintain their aircraft and a basis to construct their ANSP. In some cases, the DAH may prepare and submit instructions for continued airworthiness (ICA) containing instructions on how to maintain the aircraft onboard network system for acceptance by the responsible Aircraft Certification Service office. ICA can typically be found in the Aircraft Maintenance Manual (AMM), while other types of manufacturer-recommended maintenance instructions can be found in the Fault Isolation Manual (FIM), Service Letters (SL), and Service Bulletins (SB), to name a few. These documents will address all aspects of the related SC to ensure system integrity, security, and airworthiness for the lifespan of the aircraft.

Note: Due to the sensitive nature of the DAH's documents, all documents related to ANSP processes and procedures should be considered as Sensitive Security Information (SSI).

7.2.1 Aircraft Modifications. Aircraft modified with connectivity to a non-U.S. governmental service provider and a failure condition classification of "major" or higher require similar responsible Aircraft Certification Service office-approved instructions as part of the STC or amended TC package prior to approval for return to service.

7.2.2 Deadline. It is the responsibility of the operator to review and revise the ANSP within the timeframe specified in the ANSP authorization (generally, within 30 days of the revision date for the DAH source document). The regulatory oversight office will reissue OpSpec D301, Aircraft Network Security Program (ANSP), to reflect the revised DAH document's date.

8 WHAT OPERATOR ENTITY IS RESPONSIBLE FOR THE ANSP? Current operator infrastructure may require adjustment to accommodate the management of an ANSP. This adjustment usually necessitates a closer working relationship between aircraft avionics engineering and information technology (IT) security departments. Early experience with ANSP authorizations has found that both departments in a large operation are adequately qualified to handle an ANSP. Some operators without a dedicated IT department may need assistance from an external engineering or IT security vendor.

8.1 ANSP Oversight. In general, the FAA will require that the operator determine internal departmental responsibility for the ANSP, which should be clearly documented in the ANSP section of the manual described in paragraph 10. This section should identify a data security manager by position. The data security manager acts as the administrator for the entire ANSP process for the operator. The authorization will generally require that the operator notify the FAA in writing (typically within 5 business days) of changes to the data security manager. Ultimate responsibility for the ANSP rests with the operator seeking operational approval for an aircraft certificated with an SC.

8.2 ANSP Scope. Operators must develop and maintain an ANSP that is sufficiently comprehensive in scope and detail to accomplish the following:

1. Ensure that data security protection is sufficient to prevent access by unauthorized devices or personnel external to the aircraft.
2. Ensure that security threats specific to the operator’s fleets, routes, and maintenance practices are identified and assessed, and that risk mitigation strategies are implemented to ensure the continued airworthiness of the aircraft.
3. Prevent inadvertent or malicious changes to the aircraft network, systems, and software, including those possibly caused by maintenance activity.
4. Prevent unauthorized access from sources on board the aircraft.

Note: An operator’s ANSP should not include independent aircraft testing that tampers with the certified system. This could result in nonconformance to type design and render the aircraft unairworthy.

9 WHAT IS THE PROCESS FOR GAINING AUTHORIZATION FOR AN ANSP?

9.1 Regulatory Basis. The evolutionary integration of certain aircraft models and network-connected systems have necessitated the use of SCs for certification to mitigate identified electronic system security vulnerabilities. Due to the potential impact these designs have on an operator, OpSpec D301 is issued to promote standardization and utilization of applicable industry standards as appropriate for each operator and its aircraft, as well as DAH network security guidance provided to assist operators with maintaining conformity to the SC (refer to § 119.49(a)(14)).

9.2 Notification. An operator will notify its regulatory oversight office of its intent to operate an aircraft requiring an ANSP under the OpSpec. This notification should be made no less than 90 days prior to aircraft delivery and should address all sections of the DAH’s network security guidance documents.

9.3 Review. The applicable General Aviation or Air Carrier Safety Assurance office will collaborate with the Flight Standards Service Aircraft Maintenance Division and the FAA Office of Information and Technology (AIT) Security and Privacy Risk Management Staff to provide IT security support, assist in reviewing the submitted package, and provide concurrence prior to program authorization.

9.4 Authorization. When the review is satisfactorily completed, the Aircraft Maintenance Division will issue a letter of concurrence and recommend OpSpec D301 authorization to the regulatory oversight office. The concurrence letter will be referenced in the “Support Information Reference” box in the digital signature block of D301.

10 DO OPERATORS HAVE TO CREATE A SEPARATE MANUAL FOR THE ANSP? No. It is the operator’s prerogative to choose where it places the ANSP in its manual system. However, the manual or section of the manual where the ANSP resides must reference the operator’s D301 authorization since it is directly tied to this OpSpec.

10.1 **Operator's Manual.** It is acceptable to create a General Maintenance Manual (GMM) or General Procedures Manual (GPM) section identified as an ANSP section with references to other interfacing manuals. For example, an ANSP may interface with an operator's IT procedures, training, and airport operations manuals. These interfacing documents do not require acceptance under an FAA-authorized ANSP. However, the FAA may request to review these interfacing documents prior to acceptance, during an ANSP revision, or during routine surveillance. The operator's manual or manual section comprising the ANSP should be subject to secure storage and handling to prevent disclosure of sensitive information.

Note: Due to the sensitive nature of the operator's ANSP, all documents related to ANSP processes and procedures should be considered as SSI.

10.2 **Manual Sections.** A comprehensive manual or section should include plans and procedures for the following ANSP components:

1. A security environment description;
2. Roles and responsibilities, including persons with authority and responsibility;
3. Training/qualifications;
4. The control of portable software, data loading devices, and Ground Support Equipment (GSE) access and use;
5. The control of access to the airport's wired and wireless service network;
6. The control of access to the Loadable Software Airplane Part (LSAP) librarian resource;
7. The creation of secure parts signing processes and the control of access to private keys;
8. The control of aircraft conformity to type design;
9. The provisions for parts pooling and parts borrowing;
10. The procedures for part exchanges within the operator's own fleet;
11. Event recognition, response, reporting, and recovery; and
12. The event evaluation process, with considerations for program improvement.

11 **IS THERE A TRAINING COMPONENT TO THE ANSP?** Training all personnel involved in the ANSP is essential to the program's success. It is expected that ANSP training will vary depending on the level of involvement of personnel and the size of an operator's workforce. Due to this variation in training, it will be up to the responsible FAA oversight office to determine the adequacy of training. As a minimum, all personnel should be familiar with the procedures defined in the ANSP. IT personnel should possess skills requisite for accomplishing IT risk assessments that are traceable to industry standards.

12 **ARE THERE SPECIAL EQUIPMENT REQUIREMENTS FOR AN ANSP?** Equipment specifications related to ANSP tasks are established by the DAH. In some cases, this equipment is referred to as GSE. Due to the intended purpose, strict physical and configuration controls should be implemented for this equipment. Ensure that all confidential and aircraft-related information is securely deleted from the GSE before disposal or sending out for repair. Procedures for reporting lost equipment or equipment that may have been unaccounted for should be in the ANSP. Additionally, the ANSP should prohibit the use of personal data storage devices for transferring data intended for an aircraft or system related to the ANSP. Only operator-approved storage devices should be used to ensure secure transmission.

13 **HOW DOES THE ANSP AFFECT MAINTENANCE PROGRAMS?** Placing on-aircraft activities related to the ANSP in the maintenance program is a logical approach. Activities ranging from scheduled data integrity and software conformity checks to aircraft assigned maintenance laptop/GSE restoration and updates should be added to the maintenance program. Maintenance program tasks related to the ANSP can have an acceptance process similar to Reduced Vertical Separation Minimums (RVSM), Extended Operations (ETOPS), Lower Landing Minimums (LLM), and other OpSpecs-authorized programs. Automated downloads of security log files are not considered a maintenance task and should not be included in the maintenance program.

14 **WHAT IS DONE WITH THE SECURITY LOG FILES THAT MAY BE REQUIRED BY AN SC?** In cases where security logs are generated, operators should retain security logs extracted from the aircraft's network. The security logs relevant to airworthiness will be identified by the DAH in any established procedures developed because of an SC and may have specified transfer methods, retention times, and analytical tools mandated by those procedures or DAH manuals. Operators are expected to conduct continuous or scheduled analysis of these logs for anomalies to better understand normal system behavior and identify security risks to an extent consistent with their operational/threat profile. The ANSP should specify the frequency, methods of storage, retrieval, and analysis of the logs. In addition to scheduled download and analysis, security logs should be retained and analyzed following a National Transportation Safety Board (NTSB) reportable event that may be the result of an electronic system security event or anomaly. Current practices have found it beneficial to create duplicate log files; one file for immediate analysis, and one for unaltered history. These files should be securely transmitted and stored. One example is a secure crate: a digital container for aircraft software parts and related digital products used for electronic distribution between aerospace business partners.

15 **WHAT DOES AN OPERATOR DO IF IT SUSPECTS A SECURITY EVENT?** OpSpec D301, will, in general, require operators to conduct surveillance of their ANSP to verify compliance with the program and to identify threats to the overall system. An integral part of this surveillance is to analyze threats and report them in a form and manner consistent with the operator's IT security policies. These policies should include a method to forward relevant threats and events in compliance with TSA directives to the Cybersecurity and Infrastructure Security Agency (CISA). Documentation of this surveillance should be available in the operator's Continuing Analysis and Surveillance

System (CASS) program for technical issues, and in the operator's annual security assessment for threat information.

Note: At no time will Service Difficulty Reports (SDR) be considered an acceptable reporting method. This is due to the 96-hour reporting period.

16 **WHAT EFFECT DO MERGERS, ACQUISITIONS AND PROGRAM CHANGES HAVE ON AN ANSP?** Several activities can have a significant effect on an ANSP and may require a Principal Avionics Inspector's (PAI) review. Mergers and acquisitions must take into consideration any changes to the ANSP, especially if an acquiring operator does not have an existing program. Indepth reviews of significant changes in company interfaces are required, especially with corporate IT and flight operation entities that may have not been previously associated with an ANSP.

17 **WHAT RESPONSIBILITY DO CONTRACT MAINTENANCE PROVIDERS HAVE IN AN ANSP?** In a properly developed ANSP, a contract maintenance provider should be held to the same standards as an employee of the operator under the ANSP. Some minor differences may be allowed based on the scope of work to be performed. For example, an oncall technician at a diversion station may not require the level of training possessed by a technician employed by an Essential Maintenance Provider (EMP). Since the operator is ultimately responsible for the ANSP, any interface with critical systems by an oncall technician is under the supervision of the operator's maintenance control.

18 **RELATED READING MATERIAL.** This AC was created using information from the original RTCA DO-355 document and the current edition of DO-355, Information Security Guidance for Continuing Airworthiness. Also refer to RTCA DO-392, Information Security Event Management, regarding the handling of information security events. These RTCA documents can be found at https://my.rtca.org/nc__store. The following additional ARINC guidance can be found at https://www.aviation-ia.com/product-categories:

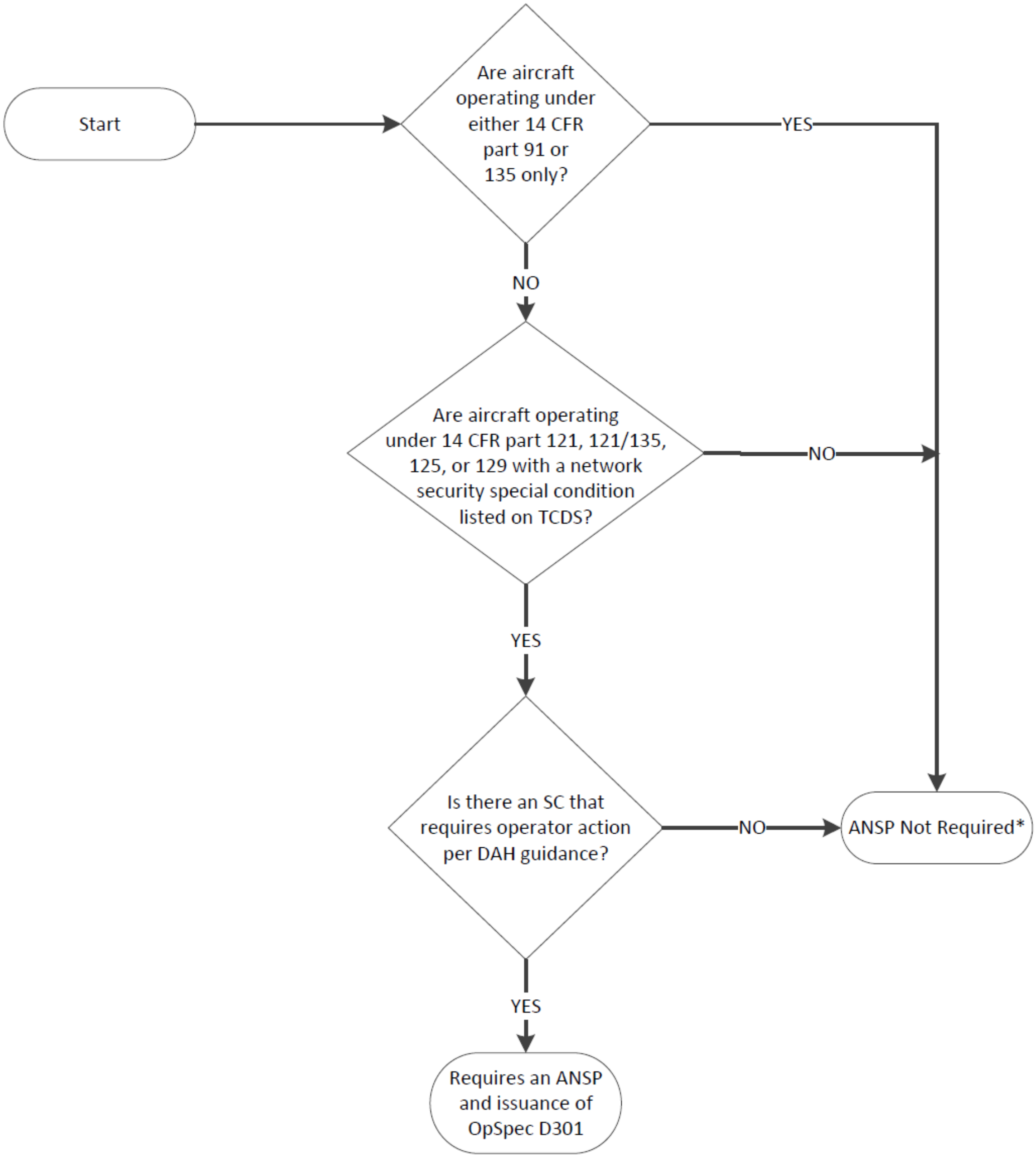
- ARINC Report 645-1, Common Terminology and Functions for Software Distribution and Loading;
- ARINC Report 665-5, Loadable Software Standards;
- ARINC Report 667-3, Guidance for the Management of Field Loadable Software;
- ARINC Report 811, Commercial Aircraft Information Security Concepts of Operation and Process Framework; and
- ARINC Report 827-1, Electronic Distribution of Software by Crate (EDS Crate).

19 AC FEEDBACK FORM. For your convenience, the AC Feedback Form is the last page of this AC. Note any deficiencies found, clarifications needed, or suggested improvements regarding the contents of this AC on the Feedback Form.

Wesley L. Mooty

Wesley L. Mooty
Acting Deputy Executive Director, Flight Standards Service

APPENDIX A. ANSP APPLICABILITY DECISION MAKING FLOWCHART


Start
Are aircraft operating under either 14 CFR part 91 or 135 only?
YES
NO
Are aircraft operating under 14 CFR part 121, 121/135, 125, or 129 with a network security special condition listed on TCDS?
NO
YES
Is there an SC that requires operator action per DAH guidance?
NO
ANSP Not Required*
YES
Requires an ANSP and issuance of OpSpec D301

*For aircraft exempt from the ANSP requirements due to operating rules: if the DAH has issued guidance related to network security requiring operator action, it must be included in the operator's program.

Advisory Circular Feedback Form

If you find an error in this AC, have recommendations for improving it, or have suggestions for new items/subjects to be added, you may let us know by contacting the Flight Standards Directives Management Officer at 9-AWA-AFB-120-Directives@faa.gov.

Subject: AC 119-1A, Operational Authorization of Aircraft Network Security Program

Date: ____________________

Please check all appropriate line items:

□ An error (procedural or typographical) has been noted in paragraph ____________ on page _______.

□ Recommend paragraph _____________ on page __________ be changed as follows:

____

____

□ In a future change to this AC, please cover the following subject:
(Briefly describe what you want added.)

____

____

□ Other comments:

____

____

□ I would like to discuss the above. Please contact me.

Submitted by: ________________________________ Date: ______________________