



U.S. Department
of Transportation

Federal Aviation
Administration

Advisory Circular

Subject: Airworthiness and Operational
Authorization of Aircraft Network
Security Program (ANSP)

Date: 9/30/15

Initiated by: AFS-300

AC No: 119-1

Change: 0

1. **WHAT IS THE PURPOSE OF THIS AC?** This advisory circular (AC) describes an acceptable means, but not the only means, of obtaining operational authorization for an aircraft certified with a special condition (SC) related to security of the onboard computer network. This AC is not mandatory and does not constitute a regulation. However, if you use the means described in the AC, you must conform to it in totality.
 2. **WHAT DOES THIS AC INTENTIONALLY EXCLUDE?** This AC does not cover physical security of the aircraft or surrounding area. Existing Federal Aviation Administration (FAA) and Transportation Safety Administration (TSA) regulations address compliance with physical security guidelines.
 3. **WHO DOES THIS AC APPLY TO?**
 - 3.1 **Operators.** 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).

Note: All other operations are still required to follow the design approval holder (DAH) instructions related to electronic system security isolation or protection created to meet a SC.
 - 3.2 **FAA.** Certificate-holding district offices (CHDO) and Regional Offices (RO) with oversight of certificate holders operating an aircraft requiring an ANSP.
 4. **WHY THE NEED FOR AN ANSP?** Previous aircraft designs utilized ARINC 429, ARINC 629 or Military Standard (MIL-STD) data buses to connect flight-critical avionics systems. Current designs have adopted several technological advances such as Internet Protocol (IP) connectivity to capitalize on speed and weight savings. This advanced technology can be found not only in new aircraft designs but also in postdelivery modifications.
 - 4.1 **Advanced Connectivity Technology Benefits.** A major benefit of advanced connectivity such as IP 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.
-

- 4.2 Potential Hazards.** 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, denial of service, or criminal activity.
- 4.3 Data Security.** The transmission of critical data affecting airworthiness to and from the aircraft necessitates the need for an ANSP. A comprehensive ANSP mitigates risk to network security onboard the aircraft, the off-airport supporting infrastructure (corporate offices), and everything in between, to include wired and wireless connectivity.
- 5. HOW DO I KNOW IF AN AIRCRAFT OPERATION NEEDS AN ANSP?** An aircraft requiring an ANSP to operate can be identified by a SC listed on the Type Certificate Data Sheet (TCDS) or, if later modified, will be identified in the Supplemental Type Certificate (STC) or Amended Type Certificate (ATC) with a SC. In any of these cases, only SCs requiring instructions to an operator or operator action would mandate the requirement for an ANSP (See Appendix A).
- 6. WHAT DOCUMENTS ARE USED TO CREATE AN ANSP?**
- 6.1 Special Condition.** A SC is a rulemaking action that is specific to an aircraft make and often concerns the use of new technology that the Code of Federal Regulations does not yet 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 a SC that will be added to the TCDS.
- 6.2 DAH Document.** The DAH will submit aircraft network security guidance for operators to the FAA Aircraft Certification Office (ACO) for approval when showing compliance with a SC requiring operator action. The network security guidance provides operators with information necessary to maintain their aircraft in compliance with the SC 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 ACO. This information can be found in the Aircraft Maintenance Manual (AMA), 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 and security for the lifespan of the aircraft.
- 6.2.1 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 ACO-approved instructions as part of the STC or amended type certificate (TC) package prior to approval for return to service.
- 6.2.2 Deadline.** It is the responsibility of the operator to review and revise the ANSP within 30 days of the revision date for the DAH source document. The regulatory oversight office

will reissue the operations specification (OpSpec) D301 to reflect the revised DAH document date.

- 7. WHAT OPERATOR ENTITY IS RESPONSIBLE FOR THE ANSP?** Current operator infrastructure may require adjustment to accommodate 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 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.
- 7.1 ANSP Oversight.** Internal departmental responsibility for the ANSP will be determined by the operator and will be clearly documented in the ANSP section of the manual described in paragraph 9. This section must identify a Data Security Manager by position. The Data Security Manager acts as the administrator for the entire ANSP process for the operator. The FAA must be notified in writing within 5 working days of changes to the Data Security Manager. Ultimate responsibility for the ANSP rests with the operator.
- 7.2 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 certificate holder's operations 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, including those possibly caused by maintenance activity.
 4. Prevent unauthorized access from sources onboard the aircraft.
- 8. WHAT IS THE PROCESS FOR GAINING AUTHORIZATION FOR AN ANSP?**
- 8.1 Notification.** An operator will notify its regulatory oversight office (the CHDO) of its intent to operate an aircraft requiring an ANSP. This notification should be made no less than 60 days prior to commencing intended operations and must address all sections of the DAH network security guidance documents.
- 8.2 Review.** The regulatory oversight office will collaborate with the Flight Standards (AFS) Aircraft Maintenance Division's Avionics Branch (AFS-360) and the Office of Information and Technology Services' (AIT) Security and Privacy Risk Management Staff (AIS-020) to provide IT security support, assist in reviewing the submitted package, and provide concurrence prior to program authorization.
- 8.3 Authorization.** When the review is satisfactorily completed, AFS-360 will issue a letter of concurrence and recommend OpSpec D301 authorization to the regulatory oversight office. The AFS-360 concurrence letter will be referenced in the "Support Information Reference" box in the digital signature block of D301.

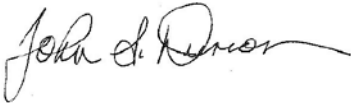
- 9. DO OPERATORS HAVE TO CREATE A SEPARATE MANUAL FOR THE ANSP?** No. It is the operator's prerogative to choose where it places the ANSP in its manual system. However, the manual or section of manual where the ANSP resides must reference the operator's D301 authorization since it is directly tied to an OpSpec.
- 9.1 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.
- 9.2 Manual Sections.** A comprehensive manual or section should include plans and procedures for the following ANSP components:
1. Roles and responsibilities, including persons with authority and responsibility;
 2. Training/qualifications;
 3. Control of maintenance laptop/ground support equipment (GSE) access and use;
 4. Control of access to airport wired and wireless service network;
 5. Controlling access to Loadable Software Airplane Part (LSAP) librarian resource;
 6. Creating secure parts signing processes and controlling access to private keys;
 7. Control of aircraft conformity to type design;
 8. Provisions for parts pooling and parts borrowing;
 9. Procedures for part exchanges within its own fleet;
 10. Event recognition and response;
 11. Event evaluation process with considerations for program improvement; and
 12. Security Environment Description.
- 10. 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 approving regulatory 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.
- 11. 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. 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.

- 12. 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 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 unless specified by the DAH in the FAA-accepted ICA.
- 13. WHAT IS DONE WITH THE SECURITY LOG FILES THAT MAY BE REQUIRED BY SC?** In cases where security logs are generated, operators are to retain security logs extracted from the aircraft's core network. Some logs may have specified transfer methods, retention times and analytical tools mandated by SC 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. 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 transmitted via a secure method. 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.
- 14. WHAT DOES AN OPERATOR DO IF IT SUSPECTS A SECURITY EVENT?** Operators are required 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 its IT security policies. These policies must include a method to forward relevant threat information to the DAH and to the Department of Homeland Security (DHS) in extreme cases. An alternative to creating a reporting infrastructure would be to participate in the Aviation Information Sharing and Analysis Center (A-ISAC). Documentation of this surveillance should be available in the operator's Continued Analysis and Surveillance System (CASS) program for technical issues, and in the operator's annual security assessment for threat information.
- 15. 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 principal avionics inspector (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. In-depth 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.

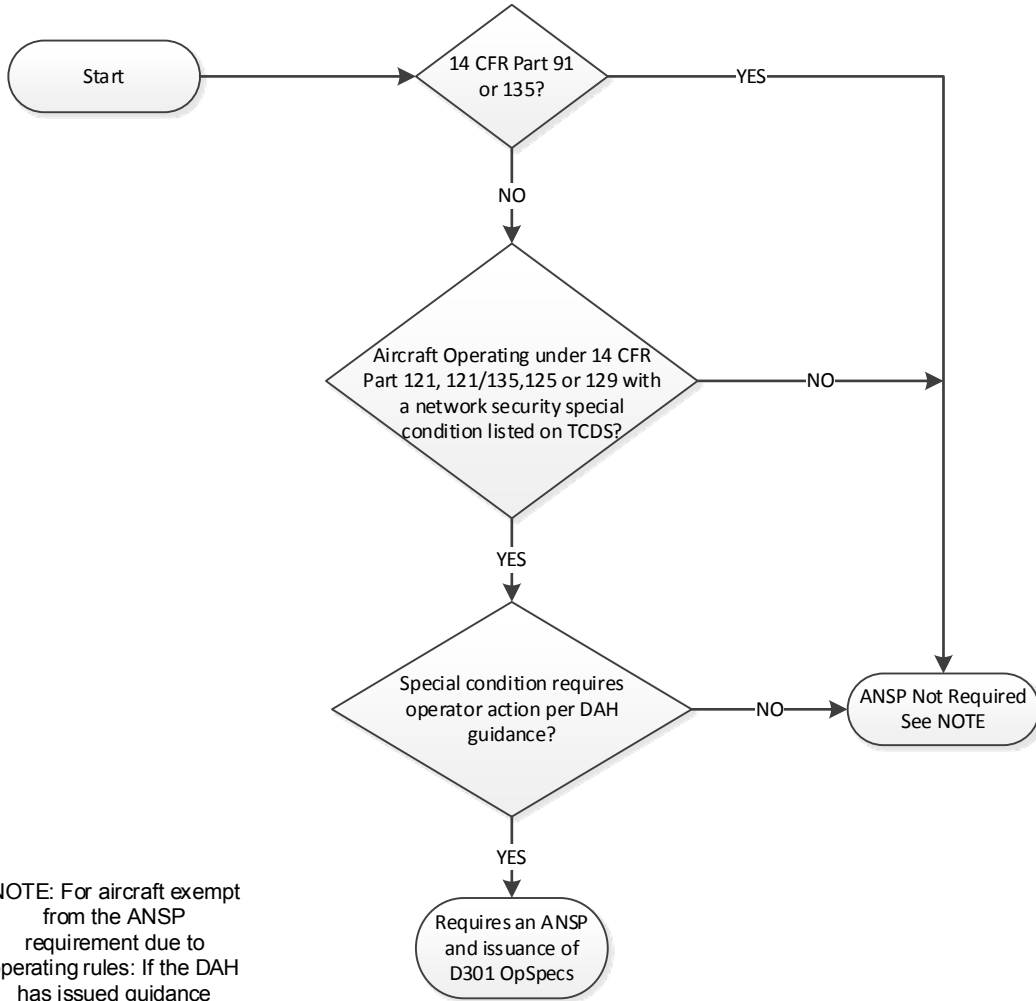
- 16. WHAT RESPONSIBILITY DO CONTRACT MAINTENANCE PROVIDERS HAVE IN AN ANSP?** In a properly developed ANSP, a contract maintenance provider should be held to the same standards as an employee of the company owning the ANSP. Some minor differences may be allowed based on the scope of work to be performed. For example, an on-call 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 on-call technician is under the supervision of the operator's maintenance control.
- 17. ARE THERE ANY RELATED DOCUMENTS I SHOULD REVIEW?** This AC was created using information from RTCA, Inc. (RTCA) document DO-355, Information Security Guidance for Continuing Airworthiness, dated June 17, 2014; ARINC Standard 811, Commercial Aircraft Information Security Concepts of Operation and Process Framework; and ARINC Standard 827, Electronic Distribution of Software by Crate. RTCA/DO-355 can be obtained at http://www.rtca.org/store_product.asp, and ARINC standards can be found at <http://store.aviation-ia.com/cf/store/>.
- 18. DOES THIS AC CANCEL ANY PRIOR ACs?** No. This is the initial AC covering the ANSP subject.
- 19. HOW CAN I GET THIS AND OTHER FAA PUBLICATIONS?** You can view a list of all ACs at http://www.faa.gov/regulations_policies/advisory_circulars/. You can view federal aviation regulations at http://www.faa.gov/regulations_policies/faa_regulations/.



John S. Duncan
Director, Flight Standards Service

APPENDIX A. ANSP FLOW CHART

A.1 ANSP Process.



NOTE: For aircraft exempt from the ANSP requirement 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 9-AWA-AFS-300-Division-Directives@faa.gov or (2) faxing it to the attention of the Avionics Branch (AFS 360) at (202) 267-1812.

Subject: AC 119-1, Airworthiness and Operational Authorization of Aircraft Network Security Program (ANSP)

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: _____