NOTICE

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

N 8900.189

National Policy

Effective Date:
5/31/12

Cancellation Date:
5/31/13

SUBJ: New OpSpec D301, Aircraft Network Security Program (ANSP)

1. Purpose of This Notice. This notice introduces a new operations specification (OpSpec) D301, Aircraft Network Security Program (ANSP), to support the operation of Next Generation (NextGen) e-Enabled aircraft.

2. Audience. The primary audience for this notice includes principal inspectors (PI) in the Flight Standards District Offices (FSDO) and certificate management offices (CMO). The secondary audience includes aviation safety inspectors (ASI) in Flight Standards Service (AFS) branches and divisions in the regions, in headquarters (HQ), and in Aircraft Evaluation Groups (AEG); PIs in the International Field Offices (IFO); and ASI course managers at the Federal Aviation Administration (FAA) Academy (AMA) Regulatory Standards Division.

3. Where You Can Find This Notice. You can find this notice on the MyFAA employee Web site at https://employees.faa.gov/tools_resources/orders_notices. Inspectors can access this notice through the Flight Standards Information Management System (FSIMS) at http://fsims.avs.faa.gov. Operators can find this notice on the FAA's Web site at http://fsims.faa.gov. This notice is available to the public at http://www.faa.gov/regulations_policies/orders_notices.

4. Background.

a. New Use of Technology. Previously, aircraft designers used aviation (ARINC 429/ARINC 629) or military standard (MIL-STD-1553) data buses to interconnect flight-critical avionics systems. Transmission Control Protocols (TCP) and/or Internet Protocols (IP) were used only to support the passenger information and entertainment systems, which were physically and logically separated from the flight-critical avionics systems. New aircraft designs use TCP/IP technology for the main aircraft backbone, connecting flight-critical avionics and passenger information and entertainment systems in a manner that virtually makes the aircraft an airborne, interconnected network domain server.

b. External System and Digital Data Bus (DDB) Access. The architecture of this airborne network may allow access to external systems and networks, such as wireless airline operations and maintenance systems, satellite communications (SATCOM), email, the World Wide Web, etc. Onboard wired and wireless devices may also have access to portions of the aircraft's DDBs that provide flight-critical functions.

c. Reasons for Aircraft Security Document. Aircraft using TCP/IP technology in this manner are commonly referred to as "e-Enabled aircraft." The design of these e-Enabled aircraft makes it difficult to maintain the certificated configuration of the aircraft without following procedures documented in an aircraft network security program (ANSP). OpSpec D301 is necessary to verify that operators have the skills, tools, and procedures in place to accomplish the requirements of the manufacturer's aircraft security document and the recommended best practices appropriate to their operations.

> **Note:** The description of e-Enabled aircraft refers to any aircraft produced or modified that require the manufacturer or design approval holder (DAH) to obtain FAA approval for the security guidance document provided to the operator; e.g., the B-787-8, B-747-8, A-350, and A-380 aircraft. (This example is not all-inclusive.)

d. Regulatory Requirements. The existing regulations did not anticipate this type of system architecture or electronic access to aircraft systems that provide flight-critical functions. Title 14 of the Code of Federal Regulations (14 CFR) and current system safety assessment policies and techniques do not address potential cyber security vulnerabilities that could be caused by unauthorized access to aircraft data buses and servers. In accordance with 14 CFR part 11, § 11.19 (as described in 14 CFR part 21, § 21.16), aircraft network systems are certificated through various means, including but not limited to type certificates (TC) and Supplemental Type Certificates (STC) that include special condition requirements (as with Boeing aircraft), and the Airworthiness Limitation Section (ALS) of the instructions for continued airworthiness (ICA) (as with Airbus aircraft).

5. New OpSpec D301. The Aircraft Maintenance Division (AFS-300) created a new OpSpec D301 for 14 CFR parts 121, 121/135, 125, and 129 that will include sections for each aircraft model, the associated manufacturer's aircraft security document, and the certificate holder's respective ANSP document.

> **Note:** OpSpec D301 applies to part 125 certificate holders and does *not* apply to 125M Letter of Deviation Authority (LODA) holders. It applies to U.S.-registered aircraft operated under part 129 and does *not* apply to part 129 operators that do not have U.S.-registered aircraft. It applies to all aircraft operated under part 129, § 129.14.

a. ANSP Authorization. The new OpSpec D301 is the means by which the principal avionics inspector (PAI) will authorize the operator's ANSP, including pertinent revisions to its Continuous Airworthiness Maintenance Program (CAMP).

b. ANSP Acceptance. PAIs are responsible for acceptance of the program with the concurrence of the other assigned PIs and the responsible Avionics Branch (AFS-360) ASI. Personnel from the Aviation Safety Information Technology Division (AQS-200) will support AFS-360 in the evaluation.

Note: Concurrence of ASIs in other specialties is required to ensure that all aspects of training are addressed and that the full impact of the e-Enabled configuration of the aircraft is assessed.

c. Meeting ANSP Requirements. Upon official notification that an operator intends to add e-Enabled aircraft or systems to their fleet, the PAI must consult AFS-360 at 202-385-4292. This will provide for early coordination to ensure that all program requirements are met prior to issuing OpSpec D301.

Note: As new e-Enabled aircraft are delivered to operators, AFS-360 is taking a proactive approach to reach out to affected PAIs to inform, educate, and assist them in initial implementation of OpSpec D301.

d. PAI Responsibility. The new OpSpec D301 requires the PAI to submit the operator's ANSP document to AFS-360 for evaluation and concurrence prior to issuance of the OpSpec. It allows the PAI to select the applicable aircraft model and to accomplish authorizations applicable to the associated manufacturer's aircraft security document and the certificate holder's associated ANSP document. Each manufacturer's listed aircraft security document will have the current revision date, document number, and name, as applicable. Each ANSP document will be identified according to the certificate holder's manual system. The PAI should select the appropriate aircraft model and insert the associated document information for the respective security program.

Table 1. OpSpec D301, Table 1—Aircraft Authorized ANSP

Aircraft M/M/S	Manufacturer's Aircraft Security Document Name and Number	Certificate Holder's ANSP
B-787-8	Boeing Doc. No. D615Z008-04, Rev. A, November 25, 2009	ABC Airlines Company Manual XYZ, Chapter 46, Section 1
B-747-8	Boeing Doc. No. D925U723-01, Original, November 11, 2011	ABC Airlines Company Manual XYZ, Chapter 46, Section 2
A-380	Airbus A380 Airworthiness Limitations Section, ALS Part 6, Aircraft Information System Security, Rev. 3, August 26, 2009	ABC Airlines Company Manual XYZ, Chapter 46, Section 3

6. Changes to Policy and Guidance. FAA Order 8900.1 is revised concurrently with the publication of this notice to include a new Volume 3, Chapter 61, Aircraft Network Security Program.

7. Action. PAIs will ensure that their assigned operators address all of the special conditions or airworthiness limitations during compliance inspections prior to accepting delivery of e-Enabled aircraft. Additionally, OpSpec D301 should be issued when the operator's ANSP is authorized, and before placing the aircraft in service.

8. Disposition. We will incorporate the information in this notice into FAA Order 8900.1 before this notice expires. Direct questions concerning the information in this notice to AFS-360 at 202-385-4292 or AFS-300 at 202-385-6435.

for 

John M. Allen
Director, Flight Standards Service

Appendix A: OpSpec D301, Aircraft Network Security Program (ANSP): 14 CFR Part 121

a. The certificate holder is authorized to conduct operations using aircraft subject to a manufacturer's FAA/CAA-approved aircraft security document provided the following conditions are met.

1. The aircraft network security program (ANSP) listed in Table 1 shall be included in the certificate holder's manual.

2. The certificate holder will implement all requirements of the manufacturer's aircraft security document, along with the recommendations appropriate to its operations.

3. The certificate holder will revise their ANSP within 30 days after the manufacturer's aircraft security document is revised.

b. ANSP Conditions and Limitations. With regards to aircraft networks, including the associated hardware, software, and information that could impact the safety and continued airworthiness of the aircraft, the ANSP must be sufficiently comprehensive in scope and detail to:

1. Ensure security protection sufficient to prevent access by unauthorized sources 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.

c. Aircraft Authorized ANSP. Each aircraft listed in Table 1 below shall be maintained in accordance with its authorized ANSP and limitations specified in these operations specifications.

Table 1—Aircraft Authorized ANSP

Aircraft M/M/S	Manufacturer's Aircraft Security Document Name and Number	Certificate Holder's ANSP
A-300-B2203	Enter manufacturer's aircraft security document name and number (e.g., Boeing Doc. No. D615Z008-04, Rev. A, November 25, 2009).	Please enter the ANSP document name and section references (e.g., ABC Airlines Company Manual XYZ, Chapter 46, Section 1).
A-319-112		
A700		
B-737-4B7		
B-757-2B7		
DC-9-81		
F-28-MK0100		

Enter optional text for nonstandard paragraph authorization.

Appendix B: OpSpec D301, Aircraft Network Security Program (ANSP): 14 CFR Part 125

a. The certificate holder is authorized to conduct operations using aircraft subject to a manufacturer's FAA/CAA-approved aircraft security document provided the following conditions are met.

1. The aircraft network security program (ANSP) listed in Table 1 shall be included in the certificate holder's manual.

2. The certificate holder will implement all requirements of the manufacturer's aircraft security document, along with the recommendations appropriate to its operations.

3. The certificate holder will revise their ANSP within 30 days after the manufacturer's aircraft security document is revised.

b. ANSP Conditions and Limitations. With regards to aircraft networks, including the associated hardware, software, and information that could impact the safety and continued airworthiness of the aircraft, the ANSP must be sufficiently comprehensive in scope and detail to:

1. Ensure security protection sufficient to prevent access by unauthorized sources 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.

c. Aircraft Authorized ANSP. Each aircraft listed in Table 1 below shall be maintained in accordance with its authorized ANSP and limitations specified in these operations specifications.

Table 1—Aircraft Authorized ANSP

Aircraft M/M/S	Manufacturer's Aircraft Security Document Name and Number	Certificate Holder's ANSP
AERSTR-RX-6	Enter manufacturer's aircraft security document name and number (e.g., Boeing Doc. No. D615Z008-04, Rev. A, November 25, 2009).	Enter the ANSP document name and section references (e.g., ABC Airlines Company Manual XYZ, Chapter 46, Section 1).
AN-AN-2		
AR-11-AC		
B-737-200		
BE-100-100		
CV-440-580STC		
MU-2B-10		

Enter optional text for nonstandard paragraph authorization.

Appendix C: OpSpec D301, Aircraft Network Security Program (ANSP): 14 CFR Part 121/135

a. The certificate holder is authorized to conduct operations using aircraft subject to a manufacturer's FAA/CAA-approved aircraft security document provided the following conditions are met.

1. The aircraft network security program (ANSP) listed in Table 1 shall be included in the certificate holder's manual.

2. The certificate holder will implement all requirements of the manufacturer's aircraft security document, along with the recommendations appropriate to its operations.

3. The certificate holder will revise their ANSP within 30 days after the manufacturer's aircraft security document is revised.

b. ANSP Conditions and Limitations. With regards to aircraft networks, including the associated hardware, software, and information that could impact the safety and continued airworthiness of the aircraft, the ANSP must be sufficiently comprehensive in scope and detail to:

1. Ensure security protection sufficient to prevent access by unauthorized sources 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.

c. Aircraft Authorized ANSP. Each aircraft listed in Table 1 below shall be maintained in accordance with its authorized ANSP and limitations specified in these operations specifications.

Table 1—Aircraft Authorized ANSP

Aircraft M/M/S	Manufacturer's Aircraft Security Document Name and Number	Certificate Holder's ANSP
AMD-20-D	Enter manufacturer's aircraft security document name and number (e.g., Boeing Doc. No. D615Z008-04, Rev. A, November 25, 2009).	Enter the ANSP document name and section references (e.g., ABC Airlines Company Manual XYZ, Chapter 46, Section 1).
B-747-246B		
B-747-469		
DC-9-15F		
DH-1040-2A		

Enter optional text for nonstandard paragraph authorization.

Appendix D: OpSpec D301, Aircraft Network Security Program (ANSP): 14 CFR Part 129

a. The foreign air carrier is authorized to conduct operations using aircraft subject to a manufacturer's FAA/CAA-approved aircraft security document provided the following conditions are met.

1. The aircraft network security program (ANSP) listed in Table 1 shall be included in the foreign air carrier's manual.

2. The foreign air carrier will implement all requirements of the manufacturer's aircraft security document, along with the recommendations appropriate to its operations.

3. The foreign air carrier will revise their ANSP within 30 days after the manufacturer's aircraft security document is revised.

b. ANSP Conditions and Limitations. With regards to aircraft networks, including the associated hardware, software, and information that could impact the safety and continued airworthiness of the aircraft, the ANSP must be sufficiently comprehensive in scope and detail to:

1. Ensure security protection sufficient to prevent access by unauthorized sources external to the aircraft.

2. Ensure that security threats specific to the foreign air carrier'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.

c. Aircraft Authorized ANSP. Each aircraft listed in Table 1 below shall be maintained in accordance with its authorized ANSP and limitations specified in these operations specifications.

Table 1—Aircraft Authorized ANSP

Aircraft M/M/S	Manufacturer's Aircraft Security Document Name and Number	Certificate Holder's ANSP
A-310-300	Enter manufacturer's aircraft security document name and number (e.g., Boeing Doc. No. D615Z008-04, Rev. A, November 25, 2009).	Enter the ANSP document name and section references (e.g., ABC Airlines Company Manual XYZ, Chapter 46, Section 1).
B-203-B		
DO-328-200		

Enter optional text for nonstandard paragraph authorization.

Appendix E: OpSpec D301, Aircraft Network Security Program (ANSP): 14 CFR Part 129, § 129.14

a. The foreign air carrier or foreign person is authorized to conduct operations using aircraft subject to a manufacturer's FAA/CAA-approved aircraft security document provided the following conditions are met.

1. The aircraft network security program (ANSP) listed in Table 1 shall be included in the foreign air carrier or foreign person's manual.

2. The foreign air carrier or foreign person will implement all requirements of the manufacturer's aircraft security document, along with the recommendations appropriate to its operations.

3. The foreign air carrier or foreign person will revise their ANSP within 30 days after the manufacturer's aircraft security document is revised.

b. ANSP Conditions and Limitations. With regards to aircraft networks, including the associated hardware, software, and information that could impact the safety and continued airworthiness of the aircraft, the ANSP must be sufficiently comprehensive in scope and detail to:

1. Ensure security protection sufficient to prevent access by unauthorized sources external to the aircraft.

2. Ensure that security threats specific to the foreign air carrier or foreign person'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.

c. Aircraft Authorized ANSP. Each aircraft listed in Table 1 below shall be maintained in accordance with its authorized ANSP and limitations specified in these operations specifications.

Table 1—Aircraft Authorized ANSP

Aircraft M/M/S	Manufacturer's Aircraft Security Document Name and Number	Certificate Holder's ANSP
A700	Enter manufacturer's aircraft security document name and number (e.g., Boeing Doc. No. D615Z008-04, Rev. A, November 25, 2009).	Enter the ANSP document name and section references (e.g., ABC Airlines Company Manual XYZ, Chapter 46, Section 1).
AR-7-S7CCM		
B-737-2N1		