U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: Software Management During Aircraft Maintenance

Date: DRAFT **AC No:** 43-216A
Initiated by: AFS-300 **Change:**

1 PURPOSE OF THIS ADVISORY CIRCULAR (AC). This AC provides guidance for developing a software management program and showing compliance with applicable regulations related to continued airworthiness when managing aircraft software during maintenance activities. This AC describes an acceptable means, but not the only means, to comply with Title 14 of the Code of Federal Regulations (14 CFR). However, if you use the means described in this AC to show compliance, you must follow it in all important respects. 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. This document is intended only to provide clarity to the public regarding existing requirements under the law or agency policies.

1.1 Limitations. This AC does not:

1.1.1 Provide relief where more stringent procedures or safeguards are specified by manufacturer instructions for continued airworthiness (ICA) or other regulatory guidance.

1.1.2 Specify software approval guidelines covered by Federal Aviation Administration (FAA) Order 8110.49, Software Approval Guidelines.

1.1.3 Give instructions for management of flight operation databases and software sometimes referred to as persistent data, authorized by Operations Specifications (OpSpecs) A025, Electronic Signatures, Electronic Recordkeeping Systems, and Electronic Manual Systems; and A061, Electronic Flight Bag (EFB) Program. Guidance for these OpSpecs is found in AC 120-78, Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals; and AC 120-76, Authorization for Use of Electronic Flight Bags. Software residing on aircraft not managed by OpSpecs A025 and A061 is subject to the guidance of this AC.

1.1.4 Specify management procedures for software referred to as Aircraft Support Data (ASD). Although the definition of ASD found in ARINC Report 675, Guidance for the Management of Aircraft Support Data, is specific to 14 CFR part 25, it may be applicable to other certification regulations. By definition, ASD is digital data that does not require airworthiness or operational approval.

2 AUDIENCE. This AC applies to aircraft operators and maintenance, repair, and overhaul (MRO) organizations.

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 43-216, Software Management During Aircraft Maintenance, dated December 20, 2017, is canceled.

5 **RELATED 14 CFR PARTS.** This AC applies to the sections of 14 CFR parts 43, 91, 121, 125, 129, 135, 137, and 145 specific to aircraft maintenance.

6 **RELATED READING MATERIAL (current editions):**

- AC 20-115, Airborne Software Development Assurance Using EUROCAE ED-12( ) and RTCA DO-178( ).
- AC 119-1, Operational Authorization of Aircraft Network Security Program (ANSP).
- AC 120-76, Authorization for Use of Electronic Flight Bags.
- AC 120-78, Electronic Signatures, Electronic Recordkeeping, and Electronic Manuals.
- FAA Order 8110.49, Software Approval Guidelines.
- ARINC Report 667-2, Guidance for the Management of Field Loadable Software.
- ARINC Report 675, Guidance for the Management of Aircraft Support Data.
- RTCA DO-178, Software Considerations in Airborne Systems and Equipment Certification.
- RTCA DO-355, Information Security Guidance for Continuing Airworthiness.
- RTCA DO-392, Information Security Event Management.
- SAE ARP4754, Guidelines for Development of Civil Aircraft and Systems.
- SAE ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment.

7 **AIRCRAFT SOFTWARE MANAGEMENT.** Modern aircraft systems rely on software to perform functions previously handled manually or by analog systems. Software integrity, security, conformity, and aircraft configuration control should be the goals of any software management program. Management tools should encompass the entire life cycle of aircraft software to include long-term storage or disposal of the aircraft or components. The aviation industry has made great strides in providing software management guidance in a changing environment. This AC recognizes RTCA DO-355 and interfacing industry guidance as acceptable sources for detailed procedures beyond the scope of this AC.

7.1 Software Sources.

7.1.1 Original Type Certificate (TC) Holder. Software that is part of the original aircraft design approval developed by the TC holder is revised by a Service Bulletin (SB) or Service Letter (SL).

7.1.2 Supplemental Type Certificate (STC) Holder. Software developed during an STC project is also revised by an SB or SL issued by the STC holder.

7.1.3 User Modifiable Software (UMS). In very limited cases, software can be created and revised by an operator based on specific needs. This form of software is developed and managed internally by an engineering entity within the operator's organization. In some cases, UMS may be developed by an outside source with the operator retaining the regulatory responsibility. This process will be detailed in the operator's manual.

7.1.4 Vendor Supplied. Vendor-supplied software is usually related to In-Flight Entertainment (IFE), navigational databases, and Terrain Awareness and Warning Systems (TAWS). This software is usually subject to frequent updates and is managed through OpSpecs, operator engineering documents, or contractual agreements with the vendor.

7.2 Software Storage.

7.2.1 Removable Media. Software can be stored, transported, and loaded from removable media. This media can be in many forms, such as floppy discs, CDs, DVDs, and flash memory devices (e.g., Secure Digital (SD)/microSD cards and USB drives). All forms of removable media, especially rewritable media, must be tightly controlled to prevent data corruption.

7.2.2 Portable Electronic Devices (PED). A PED dedicated for maintenance can be in the form of laptop computers, tablets, and portable data loaders (PDL). As with physical media, maintenance PEDs will also require tight control not only for data corruption but configuration control. These devices can be connected to the aircraft in a wired configuration or wireless when in close proximity to the aircraft.

7.2.3 Ground-Based Server. Software may reside on a ground-based server to provide a single source of readily available controlled software. Maintenance procedures requiring software should specify how to retrieve the correctly configured data from the server. Server storage is preferred in the case of remote transfer methods found in paragraph 7.3.4.

7.2.4 Automatic Test Equipment (ATE). In an appropriately rated part 145 repair station, software may reside on ATE specifically designed for diagnosis and repair of aircraft components. Procedures for control of ATE software should be specified in the Repair Station Manual (RSM) and audited by operators contracting with the repair station.

7.3 Software Transfer.

7.3.1 Physical Media Transfer. Removable media or PEDs are taken to the aircraft for loading to individual line replaceable units (LRU), or to stage software to centrally located data distribution access points on aircraft with system interconnectivity.

7.3.2 Wired Connection to PED. A popular method of software transfer is the wired PED due to its simplicity, utility, and security. A wired PED can store several software files for use on multiple systems and aircraft. Use of a wired connection reduces the electronic security considerations common with a wireless PED. However, in some instances the PED may have received the initial software with a wireless connection, introducing a possible vulnerability.

7.3.3 Wireless Connection to PED. A wireless PED connection allows for data transfer from any location on or near the target aircraft. Using a wireless connection for critical software applications may invoke specialized security measures depending on the system architecture.

7.3.4 Wireless Aircraft Connections. Some aircraft are initially certificated or modified with remote software transfer and loading capabilities. The advantage of this method is the ability to move time-sensitive updates rapidly, enhance configuration control, and minimize maintenance downtime. Security measures to prevent software corruption or tampering are built in at certification and reinforced by ICAs. Remote transfer and loading range is only limited by the type of connectivity.

7.4 State of Software.

7.4.1 Development. The process by which code is created to perform a specific function that is accurate, timely, and with repeatable results. Software must have the ability to be held in a ready state with assurance that the intended function is not degraded through time or human interaction.

7.4.2 Transfer. Moving software from one state or location to another that ensures the function is not altered intentionally or by error. For the purpose of this AC, aircraft software transfer includes all aspects of transferring from the software source (supplier) to the target aircraft onboard server or maintenance PED for immediate loading, or staging and loading.

7.4.3 Staged. Having software transferred to the target aircraft onboard server and ready for loading.

7.4.4 Loading. Software loading is the process of transferring and programming software into the target LRU or system, thus changing the aircraft's software configuration. This includes moving the software from a maintenance PED, or changing the status of the software from staged on an aircraft server to the current running configuration.

8 SOFTWARE LOADING DURING MAINTENANCE.

8.1 Maintenance Programs. Loading of software is an integral part of any maintenance program. This is especially true in modern aircraft and powerplants with advanced connectivity. Historically, very few software-related activities have been subject to the scheduled maintenance tasks reflected in a manufacturer's Maintenance Review Board Report (MRBR). However, software loading can be found in several sections of the relevant Aircraft Maintenance Manual (AMM) and engine manuals usually related to LRU replacement.

8.2 Procedures. There are various methods of receiving, storing, transporting, and loading of software. Most are specified by the TC, amended TC, or STC holder in the applicable ICAs created at the time of certification. Component manufacturers may also specify a method for loading software on LRUs when they are not installed on the aircraft. Preloading LRU software is a way to save time during nonscheduled maintenance events to avoid operational delays. For LRUs, these procedures can be found in the applicable Component Maintenance Manual (CMM) or equivalent.

8.2.1 Software Receiving. Historically, software parts have been received through an operator's receiving inspection process that is similar to other aircraft parts. This practice is common for software received as removable media and then distributed to a software management entity, usually the avionics engineering department. This practice will remain acceptable for removable media. For software received electronically, the receiving inspection process includes checking the software for authenticity and integrity using digital signature tools. In all cases, the operator's procedures should give specific details for removable media and electronic transfers, including the interaction between receiving inspection and the software management entity. The goal of a software receiving program should be to verify that the software requested meets the specifications of the operator and has not been altered during transfer.

8.2.2 Storage and Protection. Operators should have a software management process that includes adequate protections from software tampering while the software is in storage and during transfers. The process should include, but is not limited to, security controls of ground servers, removable media, PEDs, shop load tools, and all transfers between these devices and transfers to aircraft servers or onboard loaders. The use of digital signatures is noted and is a current best practice method for validating all software transfers. In addition, ensure that software file transfers within the operator's security environment occur over operator-owned and secured private networks. Ensure that external software file transfers occur over authenticated and encrypted network connections. This is required for all aircraft software whether or not electronic security special conditions (SC) or an Aircraft Network Security Program (ANSP) is required. Refer to AC 119-1 for more information on when an ANSP is applicable to an aircraft operator and how an ANSP is authorized.

8.2.2.1 Maintenance PED Control. PEDs used to store, transfer, and load aircraft software must be controlled. Operators should have procedures that mandate maintenance PEDs be used exclusively for aircraft software by authorized

individuals. In some limited and controlled cases, it is acceptable to have AMMs residing on the same device along with restricted internet access.

8.2.2.2 Removable Media. An operator should control any removable media device used for aircraft software transfer and loading. Use of personal removable media should not be allowed because it may contain files detrimental to an aircraft system.

8.2.2.3 Retirement. Special considerations should be given to aircraft or systems that are being retired to ensure private keys, software signature-checking capabilities, personal data, and proprietary information are not compromised. Frequently, parts with sensitive software and information may be reintroduced in an operator's logistics program or sold.

8.2.3 Software Transfer. The goal of an operator's procedures for software transfer should be to maintain integrity while making the software readily available. Only authorized personnel should be involved in the end-to-end transfer process. Procedures should specify which entities within the operator's company have access to aircraft software, what levels of access the personnel have, and by what means the software is transferred.

8.2.4 Loading. The loading of software should be performed only by authorized and trained personnel using procedures and equipment specified in ICA. All software loading should be followed by a verification procedure to ensure the aircraft is in the correct software configuration. This is especially important when loading software into LRUs off of the airplane, and after the LRU is installed in an aircraft. Preloading cannot be assumed to be correctly preconfigured because it cannot be assured that the preloaded LRU will get installed in a particular aircraft.

8.2.5 Configuration Control. The operator should have a software configuration control procedure to ensure each aircraft is in an airworthy condition and meets its type design. The procedure should include an emphasis on scheduling software loading to ensure timeliness for critical applications, especially in cases where software configurations are mandated by an Airworthiness Directive (AD) issued under 14 CFR part 39. The approved software configuration may vary from aircraft to aircraft due to system modification levels and operating environment. All onboard software loading procedures must include a configuration verification to ensure the latest software matches the operator's approved software configuration. A periodic configuration check is recommended at an interval aligned with, and made part of, the aircraft maintenance program. Special consideration should be given to cases where the host aircraft/system may require a different software revision level than specified by the LRU manufacturer in order to meet aircraft type design.

8.2.6 Component Handling. Aircraft are equipped with components that may require specific handling during transport, storage, repair, and decommissioning, as these components can contain sensitive or confidential information such as private keys and personal data. An example is when an aircraft is in heavy maintenance or during a modification and the

sensitive LRUs are removed to facilitate access. The LRUs should be placed in a secure location with limited access.

8.3 Training. Software ICA should be an integral part of all training programs with controls commensurate with the software's intended use. It is acceptable for this training to be included in a fleet type-specific training as an alternative to a standalone curriculum. It is recommended that any personnel involved in the development and distribution of software parts be familiar with the different design assurance levels defined in RTCA DO-178.

8.4 Software Program Evaluation. An operator's software management program should be evaluated for its effectiveness in managing, training, security, adherence to manual procedures, and configuration control. For parts 121 and 135 operators, this evaluation should be an integral part of their Continuing Analysis and Surveillance System (CASS). In all cases, a security threat analysis should be performed on a periodic basis as part of this process.

8.5 Reporting. In addition to an operator's CASS reports, any discoveries of security-related events should be reported to the operator's security department. These events should be evaluated and classified as unintentional or intentional, and assigned an appropriate risk level. It is recommended that these events be reported to the design approval holder (DAH) for further evaluation and trend analysis. Events that are classified as intentional and having a major impact may require reporting to law enforcement. RTCA DO-392 provides details for a comprehensive reporting program.

8.6 Record Entries. In almost all cases, software in installed aircraft systems is considered an aircraft part, and as such is subject to the same recordkeeping processes and controls as standard aircraft parts.

8.6.1 Regulatory Compliance. To ensure compliance with part 43, § 43.9; part 121, § 121.709(a); part 125, § 125.411(a); and part 135, § 135.443(a), documentation of software loading must be included in the aircraft maintenance record entries. The record entries should reference the source document for the software change, such as an AMM or SB.

8.6.2 Exceptions to Documentation Requirements. One specific exception provided by the regulations is in § 43.3(k) for pilot-managed aeronautical database updates. Additionally, IFE system software containing "content only" may not be considered maintenance and is therefore excepted from §§ 43.9, 121.709(a), 125.411(a), and 135.443(a). IFE "content only" software is described as movie, music, and game programs with no effect on an IFE system's intended function. This also includes software for systems that establish external connectivity for IFE content and interactive/shopping/payment portals. However, some IFE content may require operational review/approval/authorization (e.g., in cases where mandatory briefings are embedded and are the method for an operator to comply with required safety briefings).

8.6.3 Aircraft with SC. Aircraft certified with an SC related to electronic system security may have additional DAH manuals. These DAH manuals are created to fulfill the requirement of the SC in cases where the DAH is required to provide operators with additional guidance to maintain a secure configuration. These manuals range from lengthy documents that describe aircraft architecture and the interfacing support structure in detail, to a brief explanation of a task in the AMM.

8.6.3.1 Electronic System Security SCs Requiring an ANSP. Aircraft certified with electronic system security SCs and on a part 121, 121/135, or 125 Operating Certificate, or a part 129-issued OpSpec, are subject to an ANSP. Operations of this type are authorized by the issuance of OpSpec D301, Aircraft Network Security Program (ANSP). Details of an ANSP and the related management processes are found in AC 119-1.

8.6.3.2 Electronic System Security SCs Not Requiring an ANSP. Aircraft certified with electronic system security SCs, but which are not subject to an ANSP due to their Operating Certificate, are still required to comply with the electronic system security SCs, including the DAH instructions. Failure to comply with provisions of an SC may affect eligibility to retain an Airworthiness Certificate.

8.6.3.3 DAH Coordination. Operators of aircraft certified with electronic system security SCs are required to coordinate non-DAH software changes with the DAH to make sure security controls are not violated. The DAH should ensure that software installed as part of a design change does not compromise the certified aircraft systems.

9 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.

Lawrence Fields
Acting Executive Director, Flight Standards Service