Cyber Security Checklist

Note: This checklist is for aircraft component repair stations that

- Periodically install software into tooling (tooling as defined in Vocabulary below), aircraft components, or removeable media.
- Have network-connected equipment (as defined below) used in the calibration or repair of aircraft components.

If the repair station meets either of these criteria, please forward this checklist to the repair station in advance of the audit.

Vocabulary, as used in this checklist:

- Tooling: Automatic test equipment (ATE), portable data loaders (PDLs), and portable maintenance access terminals (PMATs).
- Removable Media: Floppy disks, CDs/DVDs, USB thumb drives, PCMCIA cards, Compact Flash cards, portable hard drives, or other external storage devices.
- Network-connected equipment: Tooling that has an internet protocol (IP) interface, such as Wi-Fi, Ethernet, or Cellular, and is connected to the company's network.
- DO-355A: The industry standard as defined by RTCA that provides cyber security guidance for aircraft components, tools, and software. RTCA is a United States non-profit organization that develops technical guidance for government regulatory authorities and industry, including Boeing and Airbus. ED-204A is the European equivalent to DO-355A.

A. Tooling (as defined in Vocabulary above)
   1. Is tooling physically stored in a location secured from unauthorized access? [DO-355A 5.2.3, 5.2.4] [NIST 800-53 PE-3]

2. Is there a means (e.g. roster) to identify authorized individuals allowed unsupervised access to tooling? [DO-355A 5.2.3] [NIST 800-53 PE-3, IA-4, AT-3, AT-4]

3. Does the repair station maintain a list of tooling that is network-connected, and has a documented information security review been performed for each item? [DO-355A Chapter 5] [NIST 800-53 CM-8, CA-2, CA-5, RA-7, SI-2]

4. Is newly-acquired tooling evaluated to determine whether it utilizes network connectivity and warrants inclusion in the Information Security Policy and an information security review? [DO-355A 5.2.1, 5.2.2] [NIST 800-53 CM-8, CA-2, CA-5, RA-7, SI-2]

B. Software

1. Is software that is installed onto tooling and/or aircraft components only downloaded from approved sources (e.g. the OEM or applicable air carrier) and through an authenticated, secure/encrypted connection? [DO-355A 2.1, 6.2.1, 6.2.2] [NIST 800-53 AC-3, MP-5, SR-5, SR-9, SC-8]

2. Are digital storage devices that host Automated Test Equipment (ATE) and aircraft component software protected electronically from hackers, malware, and unauthorized personnel? [DO-355A 2.2.3, 6.2.2, 6.2.4, 6.2.6, 6.2.7, 6.2.8] [NIST 800-53 AC-3, MP-2, MP-4]

3. Is physical storage of ATE and component software secured from unauthorized access? [DO-355A 2.2.4] [NIST 800-53 PE-3, MP-2]

4. Are technicians granted only the minimal access needed to perform their assigned duties on digital systems where software is hosted? [DO-355A 6.2.2] [NIST 800-53 AC-2, AC-6, CM-7, AU-6]

5. Does the facility ensure traceability of what specific software was installed to the component/ATE, when it was installed, and who installed it? [FAA AC 43-216 7.2.5, 7.6.1] [NIST 800-53 CM-3, CM-8, PM-5]

6. When installing Software to aircraft components, does the facility utilize the latest generation of secure ARINC 645-1 compliant dataloaders? [DO-355A 2.1 and ARINC 645-1] [NIST 800-53 SC-2, SC-13, SC-28]

C. Removable Media
   1. Is all information security affected removable media kept in a secure location? [DO-355A 2.2.4] [NIST 800-53 MP-2, MP-4, AC-20]

   2. Is removable media identified, labeled, and dedicated solely for aircraft components and tooling? [DO-355A 2.2.4] [NIST 800-53 MP-3]

   3. Is removable media checked to ensure it is free of malware before it is used? [DO-355A 2.2.4] [NIST 800-53 SI-3, SI-5, RA-5]

   4. Does the Information Security Policy prohibit connecting any other non-dedicated removable media to aircraft components and/or tooling? [DO-355A 2.2.4] [NIST 800-53 MP-7]

D. General
   1. Does the repair station have a documented Information Security Policy that covers Tooling, Software, and Removable Media, as defined in Vocabulary above? [DO-355A Chapters 2 & 5] [NIST 800-53 CA-2, CA-5, RA-7]

   2. Does the Information Security Policy include the secure and proper disposition of Tooling, Software and Removable Media, so that the Software is properly wiped or made physically unrecoverable? [DO-355A 2.2.4, 6.2.6] [NIST 800-53 MP-6]

   3. Items in this checklist should be documented in the repair station's operating procedures, as applicable.

For questions and feedback regarding this checklist, please contact the CASE representative listed in the CASE database for FedEx (CASE member 056).