EUROCAE

WWW.EUROCAE.NET

ED-204A

INFORMATION SECURITY GUIDANCE FOR CONTINUING AIRWORTHINESS

09/2020

SUPERSEDES ED-204

FOREWORD

1. This document was prepared jointly by EUROCAE Working Group 72 “Aeronautical System Security” and RTCA Special Committee 216 “Aeronautical System Security” and was approved by the Council of EUROCAE on 10 September 2020.
2. This document supersedes ED-204 Information Security Guidance for Continuing Airworthiness (June 2014).

   As compared with the previous version, the main changes are listed in a revision history table in APPENDIX F.
3. This document is technically identical to RTCA DO-355A Information Security Guidance for Continuing Airworthiness. Coordination has been achieved with RTCA SC-216 “Aeronautical System Security”.
4. EUROCAE, an international non-profit organisation, is the European leader in the development of worldwide recognised standards for aviation. This is achieved by utilising the expertise from our members and stakeholders across the global aviation community.
5. EUROCAE standards are developed following an open, transparent and consensus-based process, governed by process and quality management principles, which are clearly documented and is in line with the World Trade Organisation (WTO) Technical Barriers to Trade (TBT) Agreement, Annex 3 “Code of Good Practice for the Preparation, Adoption and Application of Standards”.
6. EUROCAE standards and other deliverables are recommendations and best industry practices. EUROCAE is not an official body of the European governments. EUROCAE standards are intended to complement and support the regulatory and certification framework.
7. Whilst efforts are made during the standards-development process to avoid the inclusion of proprietary information and material, some of the elements of this document may be the subject of patent, copyright or other proprietary rights. EUROCAE shall not be held responsible for identifying any such rights. Trade names and similar terms used within this document do not constitute an endorsement by EUROCAE thereof.
8. Copies of this document may be obtained from:

EUROCAE
9 – 23 rue Paul Lafargue
93200 Saint-Denis
France

Telephone: +33 1 49 46 19 65
Email: eurocae@eurocae.net
Website: www.eurocae.net

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

This document is a joint product of two industry committees: the EUROCAE Working Group WG-72, titled “Aeronautical Systems Security” and the RTCA Special Committee SC-216, also titled “Aeronautical Systems Security”. WG-72 was formed to address information security and the overall Aeronautical Information System Security (AISS) of airborne systems in conjunction with related ground systems and environment, while SC-216 was formed more specifically to address information security for certification and operation of aircraft and its systems. The guidance provided by this document is intended to constitute an Acceptable Means of Compliance for approving information security aspects of Continuing Airworthiness activities performed by Design Approval Holders and Operators.

This document provides guidance for the operation and maintenance of aircraft and for organizations and personnel involved in these tasks. It is intended to support the responsibilities of the Design Approval Holder (DAH) to obtain a valid airworthiness certificate and aircraft operators to maintain their aircraft to demonstrate that the effects on the safety of the aircraft of information security threats are confined within acceptable levels. As all information security threats may have an intentional origin, this document also covers Intentional Unauthorized Electronic Interaction (IUEI).

1.1 PURPOSE

This document is a resource for civil aviation authorities and the aviation industry when the operation and maintenance of aircraft and the effects of information security threats can affect aircraft safety. It deals with the activities that need to be performed in operation and maintenance of the aircraft related to information security threats.

This document gives also guidance that is related to operational and commercial effects (i.e. guidance that exceeds the safety-only effects).

ED-204A / DO-355A is a companion document to ED-202A / DO-326A “Airworthiness Security Process Specification” and ED-203A / DO-356A "Airworthiness Security Methods and Considerations" that support security in the development and modification part of the airworthiness process.

NOTE: *This document was developed in the European context of the European Aviation Safety Agency (EASA) Certification Specification CS-25 "Large Aeroplanes" and the United States context of Title 14 Code of Federal Regulations (14CFR) Part 25 "Transport Category Aircraft". Tailoring of this guidance may be used in other regulatory contexts including but not limited to CS-23, CS-27, CS-29, CS-E, CS-P, Part 23, Part 27, Part 29, Part 33, and Part 35.*

The most comprehensive possible area of the application of this guidance is deemed to be Large Transport Aircraft programs. However, this document does not make any assumptions about and is without prejudice to its applicability.

NOTE: *The measures proposed in this document may be subject to commercial terms between DAHs and operators. It is recommended that DAHs incorporate these elements into their commercial offers, especially for service and support related topics.*

1.2 SCOPE

ED-202A / DO-326A and ED-203A / DO-356A provide guidance in addressing airworthiness security during the aircraft product life cycle from project initiation until the aircraft Type Certificate (Amended Type Certificate, Supplemental Type Certificate and Amended Supplemental Type Certificate) is issued for the aircraft type design. In addition, it includes the handover of information about the Type Design that is necessary to ensure continuing airworthiness with respect to possible information security threats.

ED-204A / DO-355A (this document) provides guidance for the following stages of the product life cycle: operation, support, maintenance, administration, and decommissioning.

Where an organization subcontracts any activities in these stages, the organization retains the responsibility for aircraft information security (for contracted maintenance providers, refer to section 1.6.3).

A forthcoming document titled “Guidance on Information Security Event Management” (ISEM) will be jointly published by EUROCAE and RTCA. This document will provide guidance for managing security incidents and events that affect aircraft safety and it will support the existing safety event management guidance. It will provide guidance for processes, assessment and disposition, data exchanges, reporting, and other concerns that need to be performed in response to information security events.

Topics in the scope of Type Certification activities that are related to operation and maintenance of the aircraft such as Instructions for Continued Airworthiness (ICA) and security guidance documents are introduced in ED-202A / DO-326A and detailed in ED- 204A / DO-355A. In such cases ED-202A / DO-326A provides references to ED- 204A / DO-355A.

This document addresses information security risks only. The security measures to mitigate these risks are not limited to technical security measures; they may also be operational or management security measures.

Apart from the classical Instructions for Continued Airworthiness that are directly related to aircraft parts and systems, this document also provides guidance on Ground Support Equipment and Ground Support Information Systems that are related to the security of aircraft information systems and data networks as illustrated in FIGURE 1. Only Airborne software that can have effect on aircraft safety are in the scope of this document

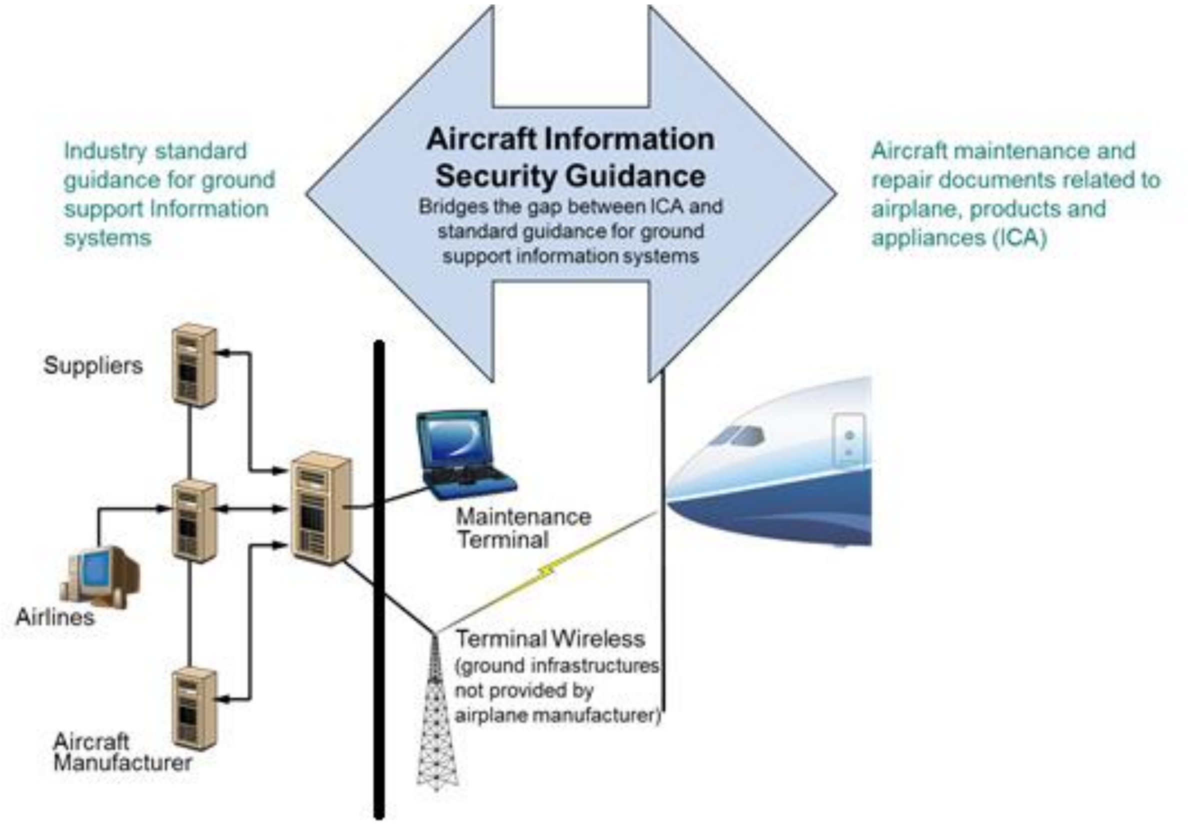
Industry standard guidance for ground support Information systems
Aircraft Information Security Guidance
Bridges the gap between ICA and standard guidance for ground support information systems
Aircraft maintenance and repair documents related to airplane, products and appliances (ICA)
Suppliers
Airlines
Aircraft Manufacturer
Maintenance Terminal
Terminal Wireless (ground infrastructures not provided by airplane manufacturer)

FIGURE 1: AIRCRAFT INFORMATION SECURITY GUIDANCE

NOTE: *The material in subsequent sections is only applicable if the aircraft and the operator use the features described.*

1.3 HOW TO USE THIS DOCUMENT

This document contains material intended to be used as Guidance Material and Acceptable Means of Compliance. The Guidance Material provides explanatory information and helps the applicant understand how to satisfy the objectives described in the Acceptable Means of Compliance in this document. Chapters X.1 and X.2 provide the Guidance Material whereas chapters X.3 and X.4 may be used as an Acceptable Means of Compliance.

This document is organized in 12 chapters plus informative appendices.

- Chapter 1 introduces the document.

The remainder of this document is organized into the following chapters and appendices. The substructure of these chapters is harmonized as follows:

- Chapter X.1 gives **General** information to introduce and define the topic
- Chapter X.2 gives an overview of what Operational Security Measures can be taken to manage the topic
- Chapter X.3 lists the Design Approval Holder (DAH) Responsibilities
- Chapter X.4 lists the Operator Responsibilities

The following topics are addressed:

Chapter 2	Airborne Software
Chapter 3	Aircraft Components
Chapter 4	Aircraft Network Access Points
Chapter 5	Ground Support Equipment
Chapter 6	Ground Support Information Systems
Chapter 7	Digital Certificates
Chapter 8	Aircraft Information Security Incident Management
Chapter 9	Operator Aircraft Information Security Program
Chapter 10	Operator Organization Risk Assessment
Chapter 11	Operator Personnel Roles and Responsibilities
Chapter 12	Operator Personnel Training

- Appendix A lists all members of the working groups that have been involved during the creation of this document.
- Appendix B contains an example Airplane Information Security Plan
- Appendix C contains an informal Glossary of Terms.
- Appendix D contains a list of acronyms.
- Appendix E contains a list of cited and relevant documents. This list is neither exhaustive nor does it characterize any of the documents therein to be applicable. However, these documents constitute a solid starting point when addressing the subject matter.
- Appendix F contains a revision history table

1.4 CONVENTIONS OF THIS DOCUMENT

Within this document, “should” is used for recommendations, “may” and “need not” are used for permission, “can” and “might not” are used for possibility, “cannot” is used for impossibility and “will” is used for an expectation arising from activities satisfying objectives from a referenced standard or regulation. The use of "must" and "shall" is avoided. Other terms that are not defined in APPENDIX B are intended to have their common dictionary meaning. This document recognizes that the guidance herein is not mandated by law, but represents a consensus of the aviation community. It also recognizes that alternative methods to the ones described herein may be available to the applicant. For these reasons, the use of words such as "shall" and "must" is avoided.

1.5 RELATIONSHIP TO OTHER DOCUMENTS

Any mention of other documents is for information only. Thus, it is expected that the cited documents are often used in the development and airworthiness certification of aircraft. A list of cited documents can be found in APPENDIX E

REFERENCES.

1.6 GENERAL CONSIDERATIONS

1.6.1 Design Approval Holder (DAH)

A Design Approval Holder (DAH) is the holder of a type certificate, a Parts Manufacturer Approval (PMA) or a Technical Standard Order (TSO) authorization or the licensee of a Type Certificate (TC) or Supplemental Type Certificate (STC).

NOTE: *All design approval holders must (source FAA):*

- *Report failures, malfunctions, and defects*
- *Make Instruction for Continued Airworthiness (including changes) available to each aircraft, aircraft engine or propeller owner*
- *Satisfy Additional Obligations for: Parts Manufacturer Approval Holder, Technical Standard Order.*

1.6.2 Instructions for Continued Airworthiness (ICA)

Instructions for Continued Airworthiness are the instructions and information that are necessary for the continued airworthiness of the aircraft, engine, propeller, parts and appliances, which are required in accordance with the applicable Certification Basis or Standard to be developed and/or referenced by the Design Approval Holder.

ICAs are not limited to the maintenance of the aircraft; they can also be operational instructions.

Specifically for maintenance, the regulatory requirements for “Instructions for Continued Airworthiness Responsibilities, Requirements, and Contents” can be found in documents provided by civil aviation regulatory systems. For example:

- EASA
  - EU 748/2012 21.A.61
  - CS 25.1529 Instructions for Continued Airworthiness
  - CS 25, Book 1, Appendix H
- FAA
  - 14 CFR Part 21.50 – Instructions for continued airworthiness and manufacturer's maintenance manuals having airworthiness limitations sections.
  - 14 CFR Part 25.1529 – Instructions for Continued Airworthiness
  - 14 CFR Appendix H to Part 25 – Instructions for Continued Airworthiness (25.1529 directs the reader to Appendix H)
- TCCA
  - CAR 521.368 Instructions for Continuing Airworthiness
  - AWM Chapter 525.1529 Instructions for Continuing Airworthiness
  - AWM Chapter 525.1529 Appendix H

The term “Instructions for Continued Airworthiness” is defined and used in a very specific way within the applicable civil aviation regulatory systems. For the definition of the term ICA, refer to the glossary. Design Approval Holders negotiate the specific content of ICA packages with the regulatory authorities. For example within the FAA system, some ICA documents are approved by the Aircraft Certification Office, but all are submitted to the FAA Aircraft Evaluation Group for acceptance or approval prior to delivery of each aircraft to an operator.

The clear intent of ICA is to provide instructions for maintenance of the aircraft, to ensure that those instructions are available within the operator's system and to ensure that the instructions are used by technicians who maintain the operator's aircraft.

NOTE: *Whenever DAH applicants use commercial parts they can refer to the guidance in FAA AC 21-45 para.5.B Commercial Parts to satisfy the regulatory requirements of 14 CFR part 21 section 21.50c.*

1.6.2.1 ICA Related to Aircraft Information Security

ICA are written to allow maintenance technicians to perform their aircraft maintenance tasks and direct them to raise items of security concern to the appropriate area of the operator's organization. It is assumed that personnel implementing ICA are not information technology (IT) security specialists.

In addition to ICA, operators may also have extensive processes, tools, facilities and information technology systems that support aircraft maintenance. As shown in FIGURE 1, DAHs provide additional non-ICA guidance to support the security of Ground Support Equipment and Ground Support Information Systems whenever they contribute to information security of the aircraft.

1.6.2.2 Differences Between ICA and Non-ICA

To summarize the difference between ICA and non-ICA operational instructions/documentation:

- ICA
  - Any required maintenance activity affecting airworthiness and safety is to be covered by an ICA.
  - ICA provide documentation of methods, inspections, processes, and procedures.
  - ICA examples: Aircraft Maintenance Manual (AMM), Maintenance Review Board Report (MRBR), Fault Isolation Manual (FIM), Trouble Shooting Manual (TSM), Airworthiness Limitation Section (ALS).
  - ICA are required to maintain the continued airworthiness of the aircraft.
- Non-ICA
  - Aircraft or ground operations affecting operation (availability, commercial aspects).
  - Off-aircraft maintenance (e.g. Shop Maintenance) is not covered by ICA.
  - Non-ICA are recommended, but not required to maintain the continuous airworthiness of the aircraft.

1.6.3 Contracted Maintenance and Service Providers

Whenever there is an arrangement between an operator and a third party such as a Maintenance Repair and Overhaul organization (MRO) or an IT service provider, it is the responsibility of the operator to ensure that this third party complies with the operator's aircraft information security requirements.

CHAPTER 2

AIRBORNE SOFTWARE

2.1 GENERAL

The objective of this section is to give guidance to ensure the authenticity and integrity of airborne software is maintained during its reception, creation, modification, storage and distribution on the ground. As deemed necessary by the DAH, confidentiality throughout the supply chain may be used to avoid reverse engineering.

Developing a Supplier Controlled Software (SCS) is part of the type design and not part of continued airworthiness. However, lifecycle security considerations of airborne software are considered.

The term airborne software as used in this document refers to all software that is carried aboard an Aircraft certified system. This includes binary applications as well as databases, firmware (including configuration of FPGAs (Field Programmable Gate Arrays) and other complex electronic hardware), and configuration files. This document addresses only airborne software that can have effect on aircraft safety.

New generation aircraft come with a large number of airborne software parts with most of them delivered in an electronic form. Operators use software tools to verify the integrity and authenticity of airborne software. Operators can deliver the software to the aircraft through several connectivity means (e.g. wired, wireless, USB-key). Operators need to ensure that the airborne software delivered to the aircraft is authorized while maintaining its integrity and authenticity. Ensuring confidentiality of software during the entire software management process may help prevent unauthorized access and reverse engineering.

For legacy aircraft, the number of airborne software parts may be lower and the variety of connectivity means may be less. Nevertheless, integrity and authenticity need to be ensured for aircraft safety. Confidentiality aspects also need to be considered to avoid reverse engineering when relevant.. If technical security measures are not possible, compensating operational and management security measures can be implemented.

Regardless of the aircraft type, operators are in transition from media-based airborne software distribution that depends on technical security measures to electronic airborne software distribution. The electronic distribution of software requires ground systems and processes that support information security.

Electronic airborne software distribution or Electronic Distribution of Software (EDS) is the process of moving software and data from one location to another location without the use of portable electronic media such as magnetic disks, optical disks, or flash drives. This classification of software distribution can make use of any data connectivity model such as wide area networks, local area networks, proprietary networks, and direct links. The connectivity method used within these models can be wired or wireless.

A common security methodology for electronic airborne software distribution is as follows.

- For electronic software distribution, integrity and authenticity are implemented by using a means of attaching one or more cryptographic signatures to the files that use a public/private key encryption method. If required, the entire software data payload may be encrypted using a public/private key method.
- Before sending a software package, a digital signature can be associated with this software package. This digital signature can only be created by the sender using its private key. The sender needs to share the associated public key. The signature is created using the contents of software, the sender’s identification information, and other related information. The recipient has the public key required to verify that the software data came from the identified sender and that nothing in the data has been altered in any way.
- Additionally, if confidentiality needs to be maintained as directed by the DAH, the sender and receiver can select and implement appropriate methods so only the

recipient can use the software package or access data within it. Encrypting a payload is one common means of ensuring confidentiality.

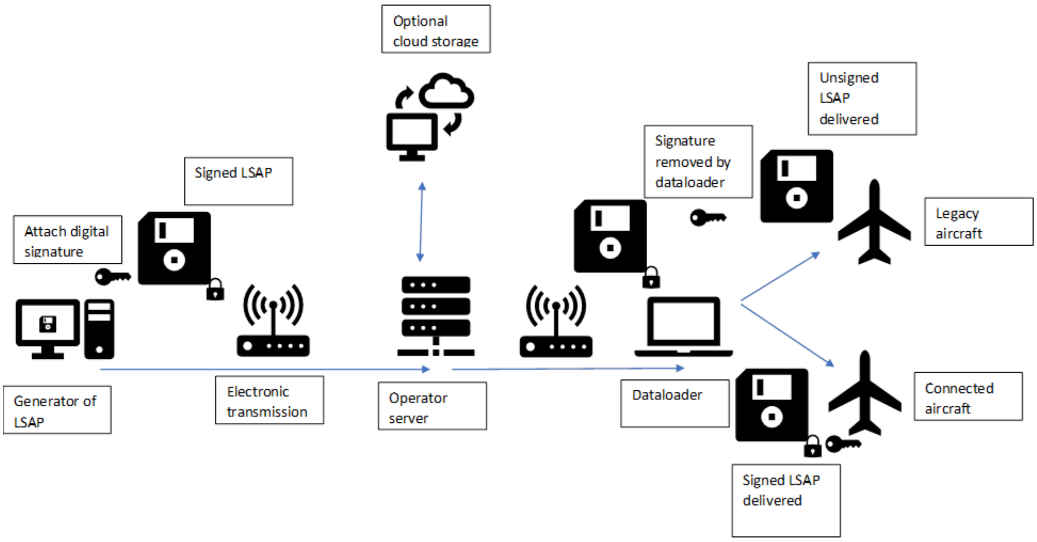

FIGURE 2: A COMMON SECURITY METHODOLOGY FOR ELECTRONIC SOFTWARE DISTRIBUTION

Refer to ARINC 667 and ARINC 827 for specific information regarding electronic distribution of airborne software.

Refer to CHAPTER 7 for specific information regarding public/private keys and the handling and management of digital certificates.

Media-based airborne software distribution uses portable electronic media. Media such as magnetic and optical disks as well as flash memory and similar media containing software and data can have a physical label attached that indicates the content information of the media.

A common security methodology for distribution of software stored on portable physical media is as follows.

- For media-based distribution, physical security is implemented by having trusted people in a physically secure environment with proper credentials prepare, label, package, and send physical media to the intended recipient.
- The media is received at the intended recipient location, checked, and processed by trusted people with proper credentials in a physically secure environment.

While this physical control process has been used extensively, it is now recommended that physical media containing airborne software also use cryptographic means as authentication and integrity mechanism.

Refer to ARINC 667 for specific information regarding physical distribution of airborne software.

NOTE: *This section addresses on-aircraft loading as well as shop loading.*

Related ARINC documents are:

- *ARINC 645 Common Terminology and Functions for Software Distribution and Loading.*
- *ARINC 667 Guidance for the Management of Field Loadable Software can provide guidance for handling of field loadable software (terms used in this section comply with ARINC 667). However, it does not cover the security of field loadable software and data.*

- *ARINC 827 Electronic Distribution of Software by Crate (EDS Crate) defines the industry standard method to be applied for electronic distribution of software.*
- *ARINC 835 Guidance for Security of Loadable Software Parts Using Digital Signatures.*

Airborne software distribution is a different process from data loading. Transferring airborne software from one location to another is software distribution. A location for distribution may include an onboard aircraft mass storage device (MSD) that is used to store software that may be loaded later. Moving airborne software into the actual onboard aircraft system components, other than a MSD, is data loading.

2.2 OPERATIONAL SECURITY MEASURES

The following subsections give an overview of what operational security measures can be taken for secure handling and managing of airborne software on the ground.

2.2.1 Reception

- Verify the authenticity and integrity of the software upon receiving. This can be done by verifying a digital signature or comparable methods, or by use of a combination of security measures to be agreed upon with the sender (aircraft manufacturer, supplier, etc.), using software tools that conform to the sender's specification.

NOTE: *A comparable method could be the usage of a sealed envelope in combination with physical media.*

- Define actions to take when software reception fails authentication or integrity checks. This would include notification to the software provider to resend the software or data. Also, include actions to take for inter-company distribution and reception authentication failures.

NOTE: *Resolve any issues with receipt of loadable software when it is received, not when it is needed.*

2.2.2 Creation/Modification

- Apply a secure process (personnel, tools) as defined in ED-202A / DO-326A and ED-203A / DO-356A and adapt the operator's environment in accordance with DAH recommendations provided in the ASOG for creating and modifying User Modifiable Software (UMS) and User Certifiable Software (UCS).

2.2.3 Storage

- During storage of airborne software on the ground, implement the security measures sufficient to prevent and detect unauthorized access in order to protect the integrity and confidentiality of the software (e.g. usage of digital signatures, encryption, locked rooms, passwords, defined roles and responsibilities, and badges).
- Ensure procedures address the full life cycle of the physical storage device (e.g. aircraft server, maintenance laptop, data loader, development computer) and the airborne software stored on it.
- Address digital certificate expiration issues that might occur during storage.
- Use encryption in addition to access controls if deemed necessary by the DAH as another layer of defense against unauthorized software access.

2.2.4 Media

- If airborne software is stored on media:
  - Ensure that the media is free of malicious code before airborne software is stored on it and have the means to verify.
  - Ensure that the media is protected from malicious code during its lifecycle and be able to verify.

- Ensure that the airborne software maintains its integrity and be able to verify.
- Consider various types of media available and the possible use restrictions and life cycle associated with each type and the possibilities of commercially installed software products (e.g. read-only media or removable media like USB mass storage devices with preinstalled applications, Secure Digital (SD) cards, compact flash cards, etc.).
- Ensure that the media is appropriately labeled (e.g. part number, version, date).
- Ensure that removable media is physically controlled.
- Treat removable media as you would portable/mobile maintenance devices.
- Whenever necessary, ensure that media content is protected against disclosure during its lifecycle, including decommissioning.

NOTE: *Depending on the selected media type, be aware that each media type bears different risks and vulnerabilities to be considered (e.g. USB mass storage device compared to read-only CD-ROM).*

2.2.5 Software Tools

- Keep equipment used for running software tools secure and free of unauthorized code, and control the configuration of this equipment. Therefore, verify the integrity and authenticity of software tools when installed in this equipment.
- These software tools include applications that run on equipment related to airborne software distribution and storage such as Portable Data Loaders (PDL's), office desktops, servers, and maintenance laptops.
- Keep equipment used for running software tools secure and free of unauthorized code, and control the configuration of this equipment.
- Ensure software tools are not used for any other purpose or in any other way than that specified by the DAH or the software supplier.
- Consider the need for management of vulnerabilities in software tools. If vulnerabilities are identified in a tool or its operating platform, determine appropriate mitigations in coordination with the tool provider. These mitigations may be technical or procedural.

NOTE: *A software supplier or DAH may specify particular security measures to be used to protect software tools. A software supplier or DAH may also specify particular security measures to be used during operation of the software tool.*

NOTE: *For additional guidance, refer to CHAPTER 5 and CHAPTER 6.*

2.2.6 Software Distribution

- Only perform transfer of airborne software by personnel who are authorized by the operator to access, manage, and store software.

  Examples of transfer within organizations:

  - Software Vault to Data Loader, Data Loader to Aircraft, and Vault to Aircraft Mass Storage.

  Examples of transfer between organizations:

  - DAH to operator, suppliers/vendors to operator or operator to MRO.
- Ensure the integrity, authenticity, and confidentiality of airborne software during transfer (physical and logical) between entities (e.g. flight ops, engineering, aircraft, airport, shop).
- Implement a chain of custody consistent with associated information security risk for transporting airborne software (record keeping) to detect information security events.

NOTE: *Airborne Software can be distributed on portable physical media or by electronic distribution. For additional guidance, refer to CHAPTER 6*

2.2.7 Data Loading

- Validate authenticity and integrity of airborne software before software loading to aircraft LRUs. This includes onboard and off aircraft software loading.
  - Ensure that airborne software is loaded as per ICA or other applicable documentation such as Component Maintenance Manual (CMM) or Service Bulletin

2.2.8 Confidentiality

- Where required, ensure that confidentiality which aims to ensure that information is not made available nor disclosed to unauthorized entities is maintained during the whole lifecycle of the airborne software (including decommissioning).
- Unauthorized disclosure of airborne software could facilitate reverse engineering. So if airborne software is distributed over open networks like the internet, use encryption techniques such as https.

2.2.9 Incident Management

- Report and investigate information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

2.3 DAH Responsibilities

The DAH will provide the security ICA and other guidance related to software distribution and data loading to the operators

NOTE: *The guidance will be based on:*

- *The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.*
- *Applicable civil aviation regulations.*

The ICA will be kept current according to 14 CFR 21.50 and EASA Reg 21.A.61.

The DAH will provide information necessary to operate the system safely and securely. This may include information on log files, where necessary.

NOTE: *Operators are required to report incidents, including security incidents. The DAH needs to provide the operators with appropriate capabilities to monitor the aircraft for incidents to support mandatory and voluntary reporting.*

2.4 OPERATOR RESPONSIBILITIES

The operator should document and implement security policies and procedures for handling and managing of airborne software distribution and data loading.

NOTE: *The operators need to demonstrate that for every aircraft in their fleet, they are able to manage the security aspects relating to safety.*

The operators should document and implement policies and procedures dependent on the risk assessment, as referenced in Chapter 10.

The operator should collect, record, and process all available logs relating to airborne software security.

NOTE: *Where logs are available for aircraft components, operators should demonstrate that they obtain the logs, record them for supporting potential incidents, and process the logs to identify events and incidents.*

CHAPTER 3

AIRCRAFT COMPONENTS

3.1 GENERAL

Regulatory requirements exist to protect aircraft components during repair and maintenance. However, aircraft information security concerns may not have been fully addressed for electronic parts.

New generation aircraft are equipped with electronic 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. Legacy aircraft may be retrofitted with connected onboard data loaders. Components loaded via these mechanisms need to be secured using similar means to that of new generation aircraft. Where an onboard data loader does not exist, the expectations on securing the storage, transport, repair, tools, and decommissioning need to be protected throughout the distribution wherever technically possible.

This section provides operational security measures to protect these components off-aircraft from unauthorized access.

3.2 OPERATIONAL SECURITY MEASURES

The following subsections provide an overview of what operational security measures can be taken for secure handling and managing of aircraft components.

3.2.1 Storage

- Secure storage of aircraft components to prevent unauthorized access.

3.2.2 Transport

- Protect aircraft components and component interfaces against physical tampering.
- Verify protection means when the aircraft component enters trusted facilities.
- Use a chain of custody for transporting aircraft components (record keeping).

3.2.3 Repair

- Secure environment (personnel, tools, and infrastructure) for repair of components.
- Ensure isolation from potentially malicious systems and storage media.

3.2.4 Tools

- Use only tools approved/recommended by the DAH or equivalent tools.
- Restrict usage of these tools to the intended purpose only.
- Keep tools in good working condition.

3.2.5 Decommissioning

- Prevent confidential data such as access key codes and passwords from recovery from aircraft components by unauthorized personnel.
- Prevent confidential data such as access key codes and passwords from transfer in case of operator change.
- Comply with procedures for disposing of aircraft parts by following the Component Maintenance Manual (CMM) or applicable civil aviation regulations.

3.2.6 Incident Management

- Report and investigate information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

3.3 DAH RESPONSIBILITIES

The DAH will provide the security ICA and other guidance related to aircraft components to the operators.

NOTE: *The guidance will be based on:*

- The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.
- Applicable civil aviation regulations.

The ICA will be kept current according to 14 CFR 21.50 and EASA Reg 21.A.61.

The DAH will provide information necessary to operate the system safely and securely. This may include information on log files, where necessary.

NOTE*:* *Operators are required to report incidents, including security incidents. The DAH needs to provide the operators with appropriate capabilities to monitor the aircraft for incidents to support mandatory and voluntary reporting.*

3.4 OPERATOR RESPONSIBILITIES

The operator should document and implement policies and procedures for the handling and managing of aircraft components regarding security.

NOTE: *The operators need to demonstrate that for every aircraft type in their fleet, they are able to manage the security aspects relating to safety.*

The operators should document and implement policies and procedures dependent on the risk assessment, as referenced in Chapter 10.

The operator should collect, record, and process all available logs relating to aircraft components security.

NOTE: *Where logs are available for aircraft components, operators should demonstrate that they obtain the logs, record them for supporting potential incidents, and process the logs to identify events and incidents.*

CHAPTER 4

AIRCRAFT NETWORK ACCESS POINTS

4.1 GENERAL

Aircraft may allow connectivity to external computer systems and networks and to passenger electronic devices. This may result in the exploitation of security vulnerabilities in aircraft systems.

Examples of areas with network access points include but are not limited to:

- Flight Deck
- Electrical/Electronics/Equipment bays
- In-Flight Entertainment and Cabin Services stations or panels
- Areas in the cabin with system interfaces
- Maintenance ports with system interfaces (inside and outside the aircraft)
- Wireless access points.

Network access points located in physically non-restricted areas need more electronic access control measures because they are difficult to physically secure against unauthorized access.

Access to restricted areas may also be controlled by various identity and access management methods or tools to further support physical security.

NOTE: *On General Aviation aircraft there might not be restricted areas due to their size and operational concept.*

4.2 OPERATIONAL SECURITY MEASURES

The following list gives an overview of what operational security measures can be taken for secure managing of aircraft access points.

- Identification and indication of network access points and restricted areas in the aircraft documentation
- Monitoring, protecting and securing of network access points and restricted areas
- Reporting and investigating information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

4.3 DAH RESPONSIBILITIES

The DAH will provide the security ICA and other guidance related to onboard network access points to the operators.

NOTE: *The guidance will be based on:*

- *The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.*
- *Applicable civil aviation regulations.*

The ICA will be kept current according to 14 CFR 21.50 and EASA Reg 21.A.61.

The DAH will provide information necessary to operate the system safely and securely. This may include information on log files, where necessary.

NOTE*:* *Operators are required to report incidents, including security incidents. The DAH needs to provide the operators with appropriate capabilities to monitor the aircraft for incidents to support mandatory and voluntary reporting.*

4.4 OPERATOR RESPONSIBILITIES

The operator should document and implement policies and procedures for the secure management of network access points regarding security.

NOTE: *The operators need to demonstrate that for every aircraft type in their fleet, they are able to manage the security aspects relating to safety.*

The operators should document and implement policies and procedures dependent on the risk assessment, as referenced in Chapter 10.

The operator should collect, record, and process all available logs relating to network access points security.

***NOTE*:** *Where logs are available for network access points, operators should demonstrate that they obtain the logs, record them for supporting potential incidents and process the logs to identify events and incidents.*

CHAPTER 5

GROUND SUPPORT EQUIPMENT (GSE)

5.1 GENERAL

This section provides guidance related to computer-based Ground Support Equipment (GSE). The term GSE, used in this section, refers to GSE that digitally connects to the aircraft system at any time during ground or maintenance operations for the purpose of data loading or as an enhancement or replacement of the on-board maintenance terminal. The following items are examples of computer-based GSE:

- COTS Laptop Maintenance Terminal (CLMT).
- Portable Maintenance Access Terminal (PMAT) if not installed as aircraft equipment by TC or STC.
- Portable Data Loader (PDL).
- Automated Test Equipment (ATE).
- System specific maintenance and troubleshooting tools and data loaders.

The usage of this GSE could adversely affect the aircraft information security when the associated risks are not properly managed.

Example risks are:

- The exploitation of software vulnerabilities in GSE could lead to the compromise of aircraft computers or software.
- Malicious software loads can be installed on aircraft computers using the GSE.
- GSE interfaces to the maintenance environment (e.g. USB, Wi-Fi, and Ethernet) can be used as a relay to get access to aircraft computers/software when connecting the GSE to aircraft equipment.
- Removable media (e.g. USB memory sticks, SD memory cards, and USB disk drives) can be used to data load or download airplane system information. Although not computer based, the use of removable media includes the use of a computer at some point in the process and has similar as well as unique potential vulnerabilities that needs to be considered. Use adequate cyber-hygiene processes to ensure that no data is recoverable from decommissioned hard drives and removable media.

This section is focused on GSE only, nevertheless some of the operational security measures may also apply to mobile devices (e.g. tablets and laptops) used for flight operational purposes that are out of scope of this document.

5.2 OPERATIONAL SECURITY MEASURES

The following subsections give an overview of what operational security measures can be taken for secure handling and managing of GSE.

5.2.1 Equipment Security and Operations Management

- Establish and apply secure procedures for delivery, storage and disposal of GSE.
- Ensure that all confidential and aircraft-related information is securely deleted from the GSE before disposal or before sending for repair.
- Ensure that only authorized mobile maintenance devices or mobile maintenance device software are used (e.g. through Tool Equipment Manual).
- Manage software and hardware configuration of GSE.
- Restrict GSE access to authorized personnel only (physical and logical including repair).
- Protect GSE against hardware and software corruption.

- Harden the system, for example through:
  - Removal of unnecessary usernames or logins
  - Disabling or removal of unnecessary services and protocols
  - Using antivirus and antispyware protection
  - Regularly applying the latest manufacturers patches
  - Removal of unneeded software and applications
  - Limit network connection to the minimum needed
  - Disable "Auto start" and similar behavior of USB and other removable media
  - Prevent booting from external media as well as unauthorized configuration modification on boot sequence
  - Use the least privilege principle (restrict access to minimum needed).
- Prevent unauthorized software being installed:
  - Equip and maintain up-to-date anti-malware and antispyware protection on the GSE. Perform regularly scheduled antivirus and antispyware checks.
  - Perform regular scheduled malware checks.
- Perform effective technical vulnerability management to identify, assess, and respond to vulnerabilities on the GSE (e.g. through the installation of security updates of the operating system) as described in ISEM.
  - Monitor threats due to technical obsolescence.

5.2.2 Access Control

- Define access rights for administrators and maintenance personnel on GSE related to their tasks.
- Restrict and protect all remote accesses to GSE.
- Restrict access to the configuration of security mechanisms to the administrator.
- Ensure the identification and authentication of each GSE administrator, prior to any administration task performed.
- Establish identity and access management processes to manage user lifecycle.
- Consider central user/account management e.g. by joining a domain controller enforcing group policies or using Mobile Device Management on all portable devices.
- Use technical means to restrict access based on pre-defined rights. This may include 2-factor authentication. If passwords are used then ensure their strength based on:
  - Balance of complexity and usability
  - Expiration period
  - Limitation of reuse.

5.2.3 Usage

- Perform aircraft maintenance activities only with GSE that is authorized for this purpose.
- Restrict usage of the GSE to maintenance purposes only.
- Restrict GSE connection only to networks and media that are authorized for maintenance purposes.
- Ensure that GSE is only used by authorized personnel.
- Report internally when GSE is lost, damaged, stolen or left unattended in a place that is not secure (refer to CHAPTER 8).

5.2.4 Storage

- Store the GSE in a maintenance organization secured zone (e.g. tool store area) or onboard aircraft with appropriate administrative and physical controls.

- Restrict access to the GSE to authorized personnel only.
- Record the transfer of GSE between maintenance personnel and the tool storage area.

5.2.5 Incident Management

Report and investigate information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

5.2.6 Lifecycle Management

Vulnerabilities in the GSE need to be managed during its lifecycle. If vulnerabilities are identified in a tool or its operating platform, determine appropriate mitigations in coordination with the tool provider. These mitigations may be technical or procedural.

5.2.7 Decommissioning

Use adequate cyber-hygiene processes to ensure that no data is recoverable from decommissioned GSE.

5.3 DAH RESPONSIBILITIES

The DAH will provide the security ICA and other guidance related to GSE to the operators.

NOTE: *Where DAH provides guidance using specific GSE equipment, the DAH recommendations are expected to be consistent with the GSE supplier's recommendations and requirements.*

The DAH should provide guidance to enable the operator to securely operate all GSE solely designed, manufactured, or sold by the DAH.

NOTE: *The guidance should be based on:*

- *The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.*
- *Applicable civil aviation regulations.*

The DAH will provide information necessary to operate the system safely and securely. This may include information on log file, where necessary.

NOTE: *Operators are required to report incidents including security incidents. The DAH needs to provide the operators with appropriate capabilities to monitor the aircraft for incidents to support mandatory and voluntary reporting.*

5.4 OPERATOR RESPONSIBILITIES

The operator should document and implement policies and procedures for the secure handling and management of GSE regarding security.

The operators should document all GSE used to connect to aircraft.

NOTE: *The operators need to demonstrate that for every aircraft type in their fleet, they are able to manage the security aspects relating to safety.*

The operators should document and implement policies and procedures dependent on the risk assessment of their operational environment as referenced in Chapter 10.

NOTE: *The risk assessment may consider available GSE supplier guidance for securing the GSE.*

The operator should collect, record, and process all available logs relating to GSE.

NOTE: *Where logs are available for GSE, operators should demonstrate that they obtain the logs, record them for supporting potential incidents, and process the logs to identify events and incidents.*

CHAPTER 6

GROUND SUPPORT INFORMATION SYSTEMS

6.1 GENERAL

Ground Support Information Systems (GSIS) are ground systems that are used to accomplish the process of Data Distribution and storage of Airborne Software and Data. Systems for creation and modification of UMS and UCS are also in the scope of Ground Support Information Systems, as described in section 2.2.2.

The objective of secure handling and managing of Ground Support Information System (GSIS) is to ensure sufficient security for all information stored in, transferred from source (e.g. aircraft or software supplier) to destination (e.g. maintenance center or aircraft / portable data loader) through GSIS to prevent information security events such as unwanted access, intrusions or service interruptions. This includes any connections that this equipment may have to other equipment connected to the GSIS and aircraft. Any connectivity to the internet and other systems can pose a significant threat to security during the transmission of software and data to and from the source and destination and needs to be assessed and protected. The implementation of adequate security for the transmission of data between ground based systems and aircraft systems helps prevent information security events from happening. Some examples of the exchange of software and data are:

- DAH and other Airborne Software suppliers to operators
- Operator’s software vault to or from Portable Data Loader mass storage
- Operator’s software vault to or from aircraft on-board mass storage
- Portable Data Loader mass storage to or from aircraft on-board mass storage
- Systems involved in shop loading.

GSIS can also include airport (e.g. wireless connectivity), MRO, and other organizations’ information systems.

NOTE: *Airborne Software is also protected by other processes referenced by CHAPTER 2).*

6.2 OPERATIONAL SECURITY MEASURES

The following subsections give an overview of what operational security measures can be taken for secure handling and managing of GSIS.

6.2.1 Connection

- Ensure security for the exchange of data between Ground Support Information Systems and aircraft
  - Prevent exposure to potentially malicious systems.

NOTE: *Using digital signature methods (e.g. ARINC 827 signed crates) to verify authenticity and integrity can reduce opportunities for tampering with airborne software.*

6.2.2 Access Control

- Role Based Access Control to be put in place to and grants appropriate privilege levels:
  - Define access rights for administrators and maintenance personnel on GSIS related to their tasks.
  - Restrict access to the configuration of security mechanisms to the administrator.
  - Ensure the identification and authentication of each GSIS administrator prior to any administration task performed.
  - Establish identity and access management processes to manage user lifecycle.
- Access Control Policy & Tools deployment needs to consider the following:

  - Restrict and protect all remote accesses to GSIS.
  - Consider central user/account management e.g. by joining a domain controller enforcing group policies or using Mobile Device Management on all portable devices.
  - If passwords are used then ensure their strength based on:
    - Balance of complexity and usability
    - Expiration period
  - Use technical means to restrict access based on pre-defined rights [shared credential, which are to be avoided as much as possible]. This may include
    - 2-factor authentication
    - Limitation of reuse
    - Expiration after a short period of time [1 year] and periodic renewal
- Use segregation of duties to authorize the use of a new file (e.g., one person performs the download and integrity check and another authorizes its use in field to mitigate the action of a single insider).

More information can be found in the ARINC document ARINC Report 645 and Supplement1 “Software Loader Security Guidance” and in NIST Special Publication 800-162 “Guide to Attribute Based Access Control (ABAC) Definition and Considerations”

6.2.3 Data Exchange

- Ensure the integrity and authenticity of the information using established standards (e.g. ARINC 823, ARINC 827 and ARINC 835).

6.2.4 System Hardening Of Ground Support Information Systems

- Harden the system, for example through:
  - Removal of unnecessary usernames or logins
  - Disabling or removal of unnecessary services and protocols
  - Using antivirus and antispyware protection
  - Regularly applying the latest manufacturers patches
  - Removal of unneeded software and applications
  - Limit network connections to the minimum needed
  - Disable "Auto start" and similar behavior of USB and other removable media
  - Prevent booting from external media as well as unauthorized configuration modification on boot sequence
  - Use the least privilege principle (restrict access to minimum needed).

NOTE: *Security agencies publish guides about hardening OS that can be used to hardening GSIS.*

6.2.5 Repair

- Ensure a secure environment (personnel, tools, and infrastructure) for repair of equipment (e.g. documented access controls to GSIS equipment and network logins).
- Ensure procedures exist to protect confidential information/data/equipment.
- Ensure that needed information is backed-up prior to repair.

6.2.6 Decommissioning

- Use adequate cyber-hygiene processes to ensure that no data is recoverable from decommissioned hard drives and removable media.

6.2.7 Incident Management

- Report and investigate information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

6.2.8 Lifecycle Management

- Consider the need for vulnerability management, as required in ED-203A / DO- 356A and ISEM, of vulnerabilities in GSIS during the lifecycle. If vulnerabilities are identified in a tool or its operating platform, determine appropriate mitigations in coordination with the tool provider. These mitigations may be technical or procedural.
- Monitor threats due to technical obsolescence.

6.3 DAH RESPONSIBILITIES

The DAH may provide the aircraft security ICA and other guidance related to GSIS to the operators.

The DAH should provide guidance to enable the operator to securely operate all GSIS solely designed, manufactured or sold by the DAH.

NOTE: *The guidance should be based on:*

- *The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.*
- *Applicable civil aviation regulations.*

6.4 OPERATOR RESPONSIBILITIES

The operator should document and implement policies and procedures for the secure handling and management of GSIS regarding security.

The operators should document all GSIS used to support the aircraft.

NOTE: *The operators need to demonstrate that for every aircraft type in their fleet, they are able to manage the security aspects relating to safety.*

The operators should document and implement policies and procedures dependent on the risk assessment of their operational environment as referenced in CHAPTER 10.

The operator should collect, record, and process all available logs relating to GSIS.

NOTE: *Where logs are available for GSIS, operators should demonstrate that they obtain the logs, record them for supporting potential incidents, and process the logs to identify events and incidents.*

CHAPTER 7

DIGITAL CERTIFICATES

7.1 GENERAL

This section covers the handling and managing of digital certificates. Public key cryptography is a technology widely used to encrypt or to digitally sign data or authenticate users or devices before opening secure communications. Throughout the aerospace industry, public key cryptography has been introduced in information systems to fulfill security requirements. Public key cryptography can only be considered trusted if it can be proved and certified that a given public key belongs to a given user (i.e. person, device, or organization). This information is called a digital certificate and is carried in a form of a ‘container’ together with the associated information.

The digital certificate is signed (authenticated) by a trusted third party who is called the Certificate Authority (CA) in a hierarchical Public Key Infrastructure (PKI). The certificate itself is simply a file, in a certain format specified in IETF RFC 3280, which has been digitally signed by the Certification Authority (CA) that issued the certificate. The CA’s signature on the digital certificate is essentially a notarization of the contents of the certificate

NOTE: *In some cases, certificates may be signed by an internal certificate authority without third party involvement. Before using such certificates, consider the advantages and disadvantages of a trusted third party CA.*

The term digital certificate used in this chapter refers to the public key and the associated private key of the digital certificate. Digital Signature uses the sender’s private key for signing the contents and the receiver uses the sender’s public key to verify the signature.

Encryption is done by the sender using the receiver public key to cipher contents. Decrypting is done by the receiver using their private key.

Digital certificates can be used to ensure the security of:

- Airborne Software
- Communication (Aircraft/Ground)
- Data generated by the aircraft (e.g. log files).

Further information can be found in:

- ARINC 823 for Datalink Security
- ARINC 842 for all digital certificates and private keys being used on and around the Aircraft
- ARINC 835 for Field Loadable Software
- ATA Spec 42, Aviation Industry Standards for Digital Information Security.
- NIST 800-57, Recommendations for Key Management.

The objective of handling and managing digital certificates is to provide a means of controlling those digital certificates (e.g. for airborne software signing and signature verification, ensuring their integrity and authenticity).

In order to sign airborne software, the aircraft operator uses a public/private key pair from a Certificate Authority.

NOTE: *This section makes no assumption on the need to use digital certificates versus other means that could be used for the same purpose. The selection of the usage of digital certificates versus other technical solutions is out of the scope of this document.*

7.2 OPERATIONAL SECURITY MEASURES

The following list gives an overview of what operational security measures can be taken for secure handling and managing of digital certificates related to the aircraft operation:

- Define allowed types of digital certificates (including the assurance level, to be consistent with underlying risk, as per ATA Spec 42 guidelines) and the different use cases.
- Define allowed certificate authority (or requirements to be fulfilled by them)
    - A certificate authority dedicated to aviation may have advantages.
- Define permitted tools used with digital certificates.
- Define roles, responsibilities and processes for the management of:
    - Expiration of digital certificates
    - Accessibility, handling and control of digital certificates
    - Trust Anchors, Whitelists, Certificate Blacklists, Certificate Revocation Lists or Online Certificate Status Protocol (OCSP)
    - Access to tools used with digital certificates
    - Certificate revocation (e.g. in case of compromise of a private key, an employee terminating employment, or non-activity)
    - Restriction of access to private keys
- Perform certificates revocation in a timely and effective manner. Evaluate the correct propagation of the revocation to all concerned assets.
- Report and investigate information security events so safety impacts can be properly understood and security can be improved in the future. Refer to CHAPTER 8.

7.3 DAH RESPONSIBILITIES

The DAH will provide the security ICA and other guidance related to digital certificates to the operators.

NOTE: *The guidance will be based on:*

- *The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.*
- *The applicable certificate policies (as defined by the certificate authority)*
- *Applicable civil aviation regulations*

The ICA will be kept current according to 14 CFR 21.50 and EASA Reg 21.A.61.

7.4 OPERATOR RESPONSIBILITIES

The operator should document and implement policies and procedures for the secure handling and management of digital certificates.

NOTE: *The operators need to demonstrate that for every aircraft type in their fleet, they are able to manage the security aspects relating to safety.*

The operators should document and implement policies and procedures dependent on the risk assessment of their operational environment as referred to in Chapter 10.

The operator should collect, record, and process all available logs relating to digital certificates.

NOTE: *Where logs are available for digital certificates, operators should demonstrate that they obtain the logs, record them for supporting potential incidents, and process the logs to identify events and incidents.*

CHAPTER 8

AIRCRAFT INFORMATION SECURITY INCIDENT MANAGEMENT

8.1 GENERAL

The content of this chapter is limited to Aircraft Information Security Incident Management and does not supersede any requirements or regulations for occurrence reporting.

The objective of Aircraft Information Security Incident Management is to ensure that information security events associated with aircraft systems are communicated in a manner allowing timely corrective action to be taken and to ensure that a consistent and effective approach is applied to the management of aircraft information security events. It is assumed that Design Approval Holders and operators operate a system for collecting, investigating, and analyzing reports of and information related to occurrences that cause or might cause adverse effects on the continued airworthiness of the aircraft. This system must comply with requirements defined by applicable civil aviation regulations (e.g. EU 748/2012 21.A.3/14 CFR 21.3 for DAH or EU 1321/2014 M.A.202/14 CFR 121.703 for operators)[1]. Whenever an information security event is assessed to have a potential impact on continuing airworthiness or aircraft safety, it needs to be managed in compliance with the above-mentioned requirements.

The detailed process on how to manage information security event management are described in ISEM “Guidance on Information Security Event Management” (Refer to 1.2).

8.2 OPERATIONAL SECURITY MEASURES

Operational security measures for information security event management are described in ISEM.

8.3 DAH RESPONSIBILITIES

Consistent with current practices regarding airworthiness, the DAH may provide guidance to the operators to establish policies and associated procedures for managing Aircraft Information Security incidents as defined in ISEM.

NOTE: *The guidance will be based on:*

- *The information security requirements that have been identified by the DAH through a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance.*
- *The operational security measures listed above (in section 8.2).*

The DAH should establish and implement a process to manage aircraft information security incidents. In case of a Security Sensitive Security Airworthiness Directive, other rules may be applicable.

If necessary, the DAH should update the Aircraft Security Operator Guidance documentation and provide it to the operators.

NOTE: *If modifications to the aircraft require an update of the Aircraft Security Operator Guidance documentation, it is covered by a process as specified in ED-202A / DO-326A.*

8.4 OPERATOR RESPONSIBILITIES

The operator should establish and implement a process to manage Aircraft Information Security Incidents as defined in ISEM.

[1] As stated in section 1.1, the most comprehensive possible area of its application is deemed to be Large Transport Aircraft programs. However, this document does not make any assumptions about and is without prejudice to its applicability.

CHAPTER 9

OPERATOR AIRCRAFT INFORMATION SECURITY PROGRAM

9.1 GENERAL

Over time, the level of digital information connectivity, network systems, and automation on the aircraft has rapidly grown, introducing new vulnerabilities to the aircraft information systems. As the usage of information and communication technology increases, aircraft information security becomes crucial. To address this need, an Aircraft Information Security Program (AISP) is necessary for guidance to document, implement, and manage key aspects of an operator's information security policy with regards to aircraft digital information transfer and connectivity.

NOTE: *The FAA Advisory Circular (AC) 119-1- Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP) describes an acceptable 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 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).*

Similarly, the Civil Aviation Safety Authority (CASA) of Australia has issued CAAP 232A-1(0) Administration of aircraft and related ground support network security programs. It provides guidance on the implementation and development of a program of aircraft information network security.

The responsibility for developing, implementing, and maintaining the AISP belongs to the operator. These security measures are discussed in the operator responsibilities section. The DAH can be relied on by the operator as a subject matter expert for items and information security events that are specialized and beyond the operator's scope of knowledge.

The main purpose of the AISP is to provide a clear approach to the operator organization on how to implement specific information security policies in a consistent and regular basis.

9.1.1 AISP Relation to ISMS

Some operators have an Information Security Management System (ISMS) that is maintained within their IT or corporate security department, which typically conforms to the ISO 27001 standard. This ISMS may be required by the company to protect its business interests or for compliance to regulatory requirements. If an ISMS exists, the processes defined in their ISMS documentation can be reviewed before creating the AISP. Many of the processes required in the AISP may already be defined in the operator's ISMS. These can be referenced from inside the AISP to avoid duplication of process elements, and to better harmonize the AISP with the ISMS documentation.

If the operator does not have an ISMS, then all of the elements in Appendix B can be considered for inclusion when developing the AISP. A common standard such as the ISO 27001 can be used, in addition to this document, as a check list for security elements to consider.

As the ISMS may have a different scope from the AISP, to distinguish between the two security processes, they can be referred to as "Operator Information Security" and "Aircraft Information Security" respectively.

While there may be much commonality between these two information security management systems, they may have different scopes and only the aspects of the ISMS that are appropriate to the aircraft technical operational requirements and constraints will be considered. When applied to the AISP, these elements will be fine-tuned to provide safety while also providing sufficient efficiency to maintain effective flight operations.

The AISP may be separate from the ISMS or may constitute a distinct section within the ISMS. One reason for having an AISP in addition to the ISMS is the differences between the aircraft information systems, and the business information systems equipment used outside of aircraft systems. While there is some overlap, the knowledge base for these two information specialty domains can have many elemental differences. Many tools, processes and procedures that are currently used in general IT are not appropriate for aircraft ground and on-board systems. One reason for having an AISP included in the ISMS is when regulatory requirements apply, mandating an ISMS to cover more safety related systems than would be covered within the AISP alone. This would allow all of the management plans – AISP and ISMS – that would require approval from the auditors to be in a single submittal document. It also would ensure consistency of in operating executing all tools, processes and procedures that are used for compliance demonstration.

As a process complementary to the ISMS process used by the operator, the AISP can be treated as a similar living document. Although the AISP complements and references the ISMS, whether it is a stand-alone document or included in the ISMS, it can be maintained by the operator’s Aircraft Information Security Center (refer to section 11.4.2). The AISP can also be oriented towards any evolving key regulatory advisories and/or restrictions that would apply to the operator.

As the AISP is only a part of the overall operator ISMS, maintaining close integration with other information security policies and teams will provide the best possible implementation of the program. The operator needs to maintain vigilance regarding the overlapping and cross-cancelling aspects of the other operator information security policies already in place by the operator, or to be put in place following the adoption of an AISP.

9.1.2 AISP RELATION TO SECURITY MANAGEMENT SYSTEM

ICAO takes measures to prevent and suppress all acts of unlawful interference against civil aviation. Standards and recommended practices (SARPs) for international aviation security are designated as Annex 17. The Aviation Security Manual (Doc 8973 – Restricted) assists contracting states in implementing Annex 17 by providing guidance on how to apply its SARPs. Chapter 9 of the Aviation Security Manual describes the Security Management System (SeMS). All operators are required to implement such a SeMS.

While the AISP is focused on all kinds of information security threats including inadvertent acts, SeMS deals with security threats against air safety with a focus on unlawful interference. Independently, the AISP could be linked to the SeMS where possible. The content of the SeMS is restricted to people with a business need to know at the operator.

As with an AISP, the Aviation Security Manual defines the following enabling elements to set up the SeMS:

- Commitment on the part of senior management to security
- Existence of an effective security policy
- Participation by employees in the development and implementation of the SeMS
- External partnerships.

The functional elements can be along the common model of plan-do-check-act.

Furthermore the SeMS follows a risk-based approach that requires a risk impact analysis, the identification and assessment of threats and risks and control strategies appropriate to the operation and type of risks.

Another item pointed out in the Aviation Security Manual is the promotion of a security culture. Security is not the responsibility of top-level management alone, but senior management assumes the overall responsibility for security.

Finally, human factors form an integral part of security, and security willingness and awareness support a robust security base.

The reason for having an AISP in addition to the SeMS is the fact that SeMS still focusses on physical security not information or cyber security.

9.2 OPERATIONAL SECURITY MEASURES

The operational security measures that need to be included in an AISP are intrinsically linked to the organization of the Operator and decisions made on the type and depth of their ISMS.

NOTE: *The structure and content of this guidance document and the guidance document from the DAH can be used for the development of an AISP.*

FAA Advisory Circular (AC) 119-1- Airworthiness and Operational Approval of Aircraft Network Security Program (ANSP) or CAAP 232A-1(0) may also serve as a reference.

9.3 DAH RESPONSIBILITIES

The DAH may provide a service to assist operator in the implementation of the recommended security measures and collect feedback for program improvements.

9.4 OPERATOR RESPONSIBILITIES

Operators should develop and document an Aircraft Information Security Program (AISP). This AISP should be:

- Documented as to how the operator will implement all requirements of the DAH's aircraft information security guidance documentation, along with the recommendations appropriate to its operations.
- Included in the relevant operator's general policies, procedures, and manuals, as required by civil aviation authorities.
- Included into the operator's corporate security processes.
- Developed to contain key components as described in this document.
- Subject to a clearly defined document management and approval process.
- Revised (and submitted for approval to the applicable civil aviation authority if required):
  - after the DAH Aircraft Security Operator Guidance (ASOG) documentation is revised within a timeframe required by the applicable civil aviation authority
  - If required by the discovery of new threats. As information security threats rapidly evolve, operators should maintain a current knowledge base on the persistent and new threats that may present themselves to the operator
  - after substantial changes in the operational environment (e.g. merger)
- Based on a risk based approach.
- Subject to a continuous improvement process.
- Consistent with an operator ISMS, if applicable, as described in section 9.1.

For the purpose of continuous improvement, the Operator should provide feedback about its compliance with the requirements of the DAH's aircraft information security guidance documentation

CHAPTER 10

OPERATOR ORGANIZATION RISK ASSESSMENT

10.1 GENERAL

The core of the AISP is the operational risk assessment. A risk-based approach, based on existing international frameworks such as ISO/IEC 31000, NIST 800-30 or ARINC 811 (which is NIST 800-30 adapted to operators) or ISO/IEC 27005 Information Security Risk Management can be developed.

10.2 OPERATIONAL SECURITY MEASURES

An operator organization risk assessment may consist of the following steps (aligned to ARINC 811):

- Identify business processes which are flight relevant and all data objects (physical and information assets) which are used in these processes
- Identify impact to airworthiness and safety concerning the aspects of confidentiality, integrity, availability
- Threat identification
- Vulnerability identification (e.g. identify if GSIS and GSE could be affected by malware)
- Level of threat determination
- Risk Determination
- Recommendations of security measures
- Risk report and risk acceptance.

The risk assessment can be integrated with the corporate risk management process to eliminate overlaps and gaps in relation to other risk assessments. However there is a need to distinguish the AISP risk assessment from the standard corporate “financial based” risk assessment.

10.3 DAH RESPONSIBILITIES

The DAH should provide the information security assumptions that have been used within a process as specified in ED-202A / DO-326A using ED-203A / DO-356A guidance to the operator.

10.4 OPERATOR RESPONSIBILITIES

Operator should consider the security assumptions provided by the DAH to perform operator's risk assessments. Operators should perform risk assessments of all systems, processes, and areas associated with aircraft information security that are part of the flight operation process. These areas include the following:

- Ground Support Information Systems (GSIS) application and operating system vulnerabilities.
- Software Distribution Processes should have adequate process checks in place to ensure authenticity of, and prevent tampering with, data and software during transfer. The complete path from software reception to the aircraft installation point needs to be considered.
- Storage of Software in Vaults has sufficient physical and electronic security in place to prevent unauthorized access.
- GSE should be managed by processes that prevent unauthorized access and usage during portable operations. GSE should be assessed for vulnerability to tampering and sabotage as well as have physical and electronic security in place to prevent unauthorized access during storage.
- Aircraft Physical Access should be reviewed to ensure only authorized personnel have access to data interface systems.

- Service providers, contracted service providers, or other third party entities should be considered as part of the risk assessment to ensure that processes and procedures provide sufficient protection from unauthorized access

This assessment should be repeated periodically and when relevant changes occur that may affect aircraft information security, such as:

- process changes,
- modifications to the aircraft systems,
- change in company culture (e.g. large employee turnover, mergers),
- new flights (e.g. other destinations, new maintenance arrangements, outsourcing)
- required to address new types of threats as they become apparent.

Confidentiality should be protected in proportion to the sensitivity of information exchanged or manipulated during the risk assessments.

NOTE: *The complexity of the risk assessment will be proportional to the size of the operator.*

CHAPTER 11

OPERATOR PERSONNEL ROLES AND RESPONSIBILITIES

11.1 GENERAL

The job roles associated with aircraft information security and the skills required for each role needs to be addressed within the operator's organization and documented within the operator's AISP.

11.2 OPERATIONAL SECURITY MEASURES

11.2.1 Skills Required for Operator Information Security Management

The tasks associated with operator aircraft information security management require various types and levels of skills and training for personnel to accomplish the necessary specific job functions.

Aircraft Information Security skills include all aspects of the entire scope of aircraft information security.

In addition to aircraft information network skills, the Aircraft Information Security Specialists need to understand how software works, algorithms, encryption, etc.

11.2.2 Aircraft Information Security Specialist

Some job roles require a deep understanding of the technical details of information security events. This is especially true for personnel that have to evaluate situations for digital threat risks, design internal digital security management procedures, and oversee the organization's macro structure for aircraft information security processes.

The functional name of such a person would be an Aircraft Information Security Specialist. It would be advisable that such persons have a combination of disciplines:

- They have a background and understanding of Information Technology (IT) security techniques and aspects.
- They also have at least a general background in the functionality of aircraft avionics systems.
- They have an understanding how software works, algorithms, encryption, etc. as applied to networking systems and avionics systems. This includes how security and integrity is accomplished at the IT network level, avionics network level, and avionics system level. This includes avionics system processes such as "data loading".
- They have basic knowledge of operating system design and configuration, software design, network operation and common programming languages, professional knowledge of network security concepts, software security concepts, identity management, log management, incident management, risk management, access control, cryptography, malware protection, digital forensics, and security intrusion tests.
- They also have experience and a clear understanding of general operator aircraft operational requirements.
- They understand the regulatory requirements that are associated with aircraft operations.
- They are capable of evaluating information security events for severity, overseeing aircraft information security programs, and responding to real time issues regarding aircraft security by communication with all effected groups within and outside the operator organization, and to the DAH if necessary.

NOTE: *The above-mentioned items are not an all-inclusive and need to be tailored according to the complexity of the operational environment.*

In large and complex operational environments, it will be necessary to have a team of people covering these disciplines since the required scope and level of detail will be too great for any one individual to cover adequately.

Examples of tasks that require an Aircraft Information Security Specialist:

- Evaluate incidents to determine the severity of an information security event.
- Evaluate security log files for indications of security incidents.
- Develop and perform risk assessments.
- Protect the aircraft software systems against information security attack. Done by the following:
  - Personnel that evaluate the need for additional security measures required within their organization.
  - Personnel that evaluate the need for additional technical security measures from the DAH.

11.2.3 Specific Task Skills

There are several security sensitive tasks that need to be performed by personnel requiring a general understanding of aircraft information security. It is advisable that all such personnel have a general background and experience with aircraft operations in an operator environment. For personnel that perform maintenance operations that are security sensitive, aircraft systems training is required. Some of the specific tasks that require specialized skills may be:

- Processing aircraft security log files in a consistent way that conforms to an accepted standard which includes:
  - Downloading aircraft security log files from the aircraft to the GSIS.
  - Aircraft security log files storage equipment maintenance.
- Analysis of aircraft security log files (this task might require the aircraft information security specialist or DAH involvement)
- Maintenance laptop and aircraft data loader usage.
- Maintenance laptop and aircraft data loader maintenance.
- Maintenance laptop and aircraft data loader software configuration management.
- Formal incident management and escalation response process.

These types of skills can be acquired primarily by operator-provided specific training plan (refer to CHAPTER 12).

The following are task skills related to security log file management:

- Use of security logs in support of regular maintenance activities (where “airline policies” are called out in the AMM/FIM)
- Use of security log files in support of specific maintenance messages (e.g., expiration of certificates)
- Retention of security log files in compliance to regulations.
- Use of security log files in support of security related investigations.
- Use of security log files for characterizing normal system behaviors and for flagging unusual behaviors.

Processes to support these task skills and use of associated tools can be defined in the operator’s AISP.

11.3 DAH RESPONSIBILITIES

As the subject matter expert on specialized systems, the DAH should recommend any necessary training and skills for performing specific job functions.

11.4 OPERATOR RESPONSIBILITIES

11.4.1 General

The operator should ensure that roles and responsibilities are documented as part of the AISP and in place to address all items in the operational security measures section. They should ensure that qualified personnel with adequate experience related to their job role are in place to satisfy all roles and responsibilities referenced in the operational security measures section.

11.4.2 Aircraft Information Security Center

Operators should have a group of skilled personnel, i.e. Aircraft Information Security Specialists. They should be organized into a group[2] such as an Aircraft Information Security Center. The Aircraft Information Security Center may be contained within the operator's IT department, corporate security, or the maintenance and engineering domain but needs to maintain formal lines of communication with all these functions.

The Aircraft Information Security Center should act as the operator's point of contact for aircraft information security events from within and outside the operator's organization.

NOTE: *In some cases, this capacity may be addressed by a sub-contractor instead of the operator itself**.***

[2] This document does not make an assumption about the size of this group. Depending on the operator it may be one person only.

CHAPTER 12

OPERATOR PERSONNEL TRAINING

12.1 GENERAL

This chapter gives guidance on aircraft information security aspects of operator personnel training.

12.2 OPERATIONAL SECURITY MEASURES

12.2.1 Training, Awareness, and Competence

It is necessary to ensure that all personnel who are assigned responsibilities defined in the AISP are competent to perform the required tasks by:

- Determining the necessary competencies for personnel performing work effecting the AISP
- Providing training and documentation for each specific task that is to be performed relating to the AISP
- Evaluating the effectiveness of the actions taken
- Maintaining records of education, training, skills, experience and qualifications. Use applicable regulatory requirements to implement control of these records.

All relevant personnel need to be aware of the relevance and importance of their information security activities and how they contribute to the achievement of the AISP objectives.

- It is advisable that all employees of the organization, contractors, and third party users receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

12.2.2 Education and Certification

There is no one source of international education or certification that applies to all of the elements of the skill set needed for aircraft information security. It is advisable that each organization choose personnel based on their mixture of education, training, experience, and evidence of didactic pursuits.

It is advisable that educational and exam requirements for each security related job role be set by each operator and included in their AISP document.

12.3 DAH RESPONSIBILITIES

The DAH may prepare and offer training programs, manuals, and technical support for any specialized equipment that is solely designed, manufactured, or sold by the DAH; and where such does not exist in the general aircraft systems and IT security common body of knowledge.

12.4 OPERATOR RESPONSIBILITIES

12.4.1 Training Organization

The operator should have appropriate training for their employees. The operator may have an internal training resources department within their organization that can develop aircraft information security training within a scope that is specific to each class of job role that require it. If the operator does not have a training resource department, or chooses not to develop training internally, training resources may be solicited from an outside source that is capable of supplying adequate training.

This chapter describes elements of training that should be required for both internal and external training resources.

12.4.2 Scope of Training (General and Specific)

Training programs should be developed to cultivate awareness of aircraft information security within the operator organization. Information security procedures should be clearly defined and associated with all relevant job roles. Operators should use guidance from the appropriate DAH when available, and request additional DAH guidance when necessary.

Two general categories of training should be made available within the operator organization: General security training or specific security training.

General training is for fostering the awareness of aircraft information security events within the industry for a wider group of personnel than specific training. This group includes personnel that work with security sensitive ground systems and with aircraft, but who do not have a job function that is directly related to aircraft information security.

Specific training is designed for various specific job roles directly related to aircraft information security. It is for conveying policies, procedures, technical information, and job role goals to personnel with specific security related job functions.

When the organization has training resources, they may choose to develop courses internal to the organization. However, operators may use training that has been developed by an external outside source.

Training can be delivered through various methods that make use of available technology and resources. The following is a partial list of training course delivery methods.

- Internally or externally developed training classroom mode courses
- Internally or externally developed Computer Based Training (CBT)
- Any other adequate mode of training making use of available technology, personnel, and resources.

12.4.3 General Training

General training for all personnel within the organization that are exposed to equipment (aircraft, GSE, GSIS, etc.) that have information security events should include the following:

- The need to foster a culture of information security awareness within the operator’s organization.
- Awareness training of information security risks and how they relate to aircraft safety.
- Physical Security related to information security
  - Access to digital access ports on aircraft that involve physical locks.
- Physical protection of digital and physical assets
  - Storage of equipment such as GSE in secure areas. Such equipment should be tracked through a process of checking in and out of the equipment storehouse.
- Restricted access to sensitive areas
  - Only personnel with proper credentials presented should be allowed access to areas exposed to digital security risks. For example, IDs should be visible.
- Why it is necessary to devote attention and resources to aircraft information security
  - Show examples of how security violations can cause concerns about willful tampering with proper operation of aircraft.
  - In today’s information technology environment, much of the sensitive aircraft related information that was once secured by controlling paper media is now potentially exposed to a broader range of personnel if security measures are not in place.
  - Malware can be expected to become ever more sophisticated and dangerous.

Examples of current information security events to support the general training may be acquired from different sources:

- News
  - Some information on attacks on IT systems or industrial control systems with criminal, espionage or terrorist intent are publicly available in mass media or specific security-related news channels.
- Special Interest Groups
  - Information Sharing and Analysis Centers, Working Groups, forums or associations of incident response and security teams provide relevant information to their members.
- Design Approval Holder
  - Information and guidance provided by the Design Approval Holder contains information related to the product.
- Corporate Security
  - Reported security incidents and results of risk assessments contain information that is directly related to the operational environment.
- Governmental Agencies
  - Providing alerts, advisories and bulletins

NOTE: *Before using information related to security risks or information security events in training material, confidentiality aspects should be considered to ensure that security is not jeopardized by disclosing this kind of information to a broader audience.*

Training should include guidance for maintaining security in different areas of the organization. These areas include:

- On board aircraft
  - Operator personnel should be aware of vulnerable data load access points.
- At workstations that manipulate (store, process, send or receive) software or data that is transferred to or from the aircraft
  - Enforce limited access to workstation
  - Log off or lock workstations when not present.
- GSE
  - Explain what types of GSE digitally interface to the aircraft and why they should be monitored
  - Make sure equipment is electronically secure by logging off if appropriate
  - Keep a log of equipment’s location and report if missing.
- Communicate that there are specified personnel who have been granted access to security sensitive systems or processes. They are assigned to perform specific security management tasks. Identify which digital security aspects (especially those related to physical security) fall within those persons’ job roles. Show that everyone within the organization should be alert to possible security violations and should be aware of how to recognize them.

12.4.4 Specific Training

The operator should convey the specific tasks required for each job role related to information security. This training should be specific to each security related job function.

Specific training applies to personnel having job roles that are directly related to aircraft security. This training is for personnel that directly interact with information security processes and equipment and should be developed and/or provided by the operator. This training should be based on, or derived from, guidance and recommendations provided by the DAH and the topics mentioned in the preceding chapters of this document. Such training should be designed to address the specific issues related to the job role of the person.

Some examples of security-related job roles, personnel and associated tasks are:

- Aircraft Data Ground Stations
  - Personnel responsible for the security of ground station equipment such as software vaults and terminals.
- GSE (that digitally connects to the aircraft)
  - Personnel responsible for the security of GSE.
  - This includes personnel that use GSE on a regular basis. Such personnel should have training that describes the checkout and check-in process.
    - The operator should maintain proper training for using and maintaining GSE.
    - GSE users should receive training to ensure that they are sufficiently competent to perform their assigned tasks.
    - GSE users should receive regular awareness training concerning the security aspects of their role regarding GSE.
- Security Incident Management
  - Personnel that perform security incident management functions. Training to describe the process of security incident reporting including how to report findings. The designated aircraft information security center should be the responsible area for aircraft security incident management.
- Airborne Software Reception
  - Personnel that receive and process digitally signed software parts and data. Training for the use of ground equipment and processes for checking software part integrity.
- Airborne Software Load Creation
  - Personnel that create and distribute airborne software parts and data. This applies to UMS and UCS.
- Download Aircraft Log Files
  - Personnel that download security log files from the aircraft systems should have training for using maintenance laptop, or other equipment. They need to know how and where to upload log files.
- Log File Storage
  - Personnel that retain and store security log files. Training in the use of ground information station equipment and storage management procedures.
- Log File Analysis
  - Personnel that analyze security log files. This should be done by an aircraft information security specialist who has training and experience in information technology security analysis.
- Security Management
  - Management and engineering personnel that require a 360 degree overview of aircraft information security within their organization and within the operator aircraft industry.
- Regulatory Requirements
  - Specific training should include regulatory awareness training associated with information security events and their potential effect related to the job role.
- Aircraft Information Security Specialist
  - Some of these functions will require personnel with IT security background knowledge in addition to operator in-house training.
- Digital Certificate Usage
  - ARINC 842 “Guidance for Usage of Digital Certificates” can be referenced for specific in depth information regarding aircraft digital security.

Training should include the task skills related to security log file management mentioned in section 11.2.3.

12.4.5 Training Records

Training records should be maintained, retained, and kept up to date for all personnel that receive security training according to applicable regulatory requirements.

12.4.6 Regulatory Requirements for Operator Training

Communicate all regulatory requirements that may apply to all specific job roles.

Training requirements for some specific job roles may be defined in regulatory documents such as the following:

- 14 CFR 121.375, EU 1321/2014 Part-147, EU 1321/2014 Part-66.

12.4.7 Recurrent Training

Establish and document recurrent training policies that apply to each specific job role and for general category of job role. Be sure to comply with all regulatory requirements for operator training.

Recurrent training for aircraft information security should include new technologies, system installations, new identified threats, new company procedures, etc.

12.4.8 Organizational Communication regarding Aircraft Information Security

- Establish handoff and communication processes for each role. Each operator’s organization will develop their own specific processes. Some examples follow:
    - Aircraft Maintenance may notify the IT security department
    - Aircraft Maintenance may notify Quality Assurance
    - IT Department personnel may advise Quality Assurance
    - Quality Assurance may notify the DAH
    - IT security department may advise Aircraft Maintenance.
    - Flight and cabin crew may notify Aircraft Maintenance and Flight Operations Departments.
- Establish communication processes for information security events and how they are evaluated.

    Explain the formal escalation process to handle information security events. Explain communication through chain of personnel and/or departments for reporting.

APPENDIX A

WG-72 / SC-216 MEMBERSHIP

Chairpersons:

EUROCAE WG-72	Cyrille Rosay	EASA
WG-72 SG-4	Judicael Gros-Désirs	AIRBUS
RTCA SC-216	David Pierce	GE Aviation

Secretaries:

WG-72	Clive Goodchild	BAE Systems
WG-72 SG-4	Frédérique Dauvillaire	Thales Group
SC-216	Sam Masri	Honeywell International, Inc.

Technical Programme Manager

EUROCAE	Anna Guégan

Program Director

RTCA	Karan Hofmann

Document Editors:

WG-72 SG-4	Kai Florian Tschakert	Lufthansa Technik AG
WG-72 SG-4		
SC-216	Mark Kelley	AVISTA, Inc

WG-72 SC-216 Membership -- Editorial Group*

First Name	Last Name	Company
Hannes	Alparslan	European Defence Agency (EDA)
Yohannes	Amare	The Boeing Company
Rosemberg	Andre da Silva	Agência Nacional de Aviação Civil (ANAC-Brazil)
John	Angermayer*	The MITRE Corporation
Cyrille	Aubergier	SITAONAIR
Steven	Bates	Panasonic Avionics Corporation
Cristian	Bertoldi	AIRBUS SAS
Raphael	Blaize	APSYS
György	Blazsovszky	HungaroControl
Timo	Blunck	EUROCONTROL
Andy	Boff*	Helios - UK (EUROCAE Member)
Liz	Brandli	Federal Aviation Administration (FAA)
Angelo	Bruno	LEONARDO SpA
Martin	Call	The Boeing Company

Jeffrey	Campbell	Department of National Defence of Canada
Cláudio	Castro*	EMBRAER
Stephane	CHOPART	Airbus Helicopters
Philip	Church	Helios
Ernie	Condon	National Institute for Aviation Research (NIAR) at Wichita State University
Rosemberg	da Silva	ANAC - SAE
Brian	Daly	Transport Canada
Aharon	David	A.D.Ventures Software ltd.
Peter	Davis	CAA/SRG
Claudio	de Castro	Embraer
Gilles	Descargues	Thales Group
Alexander	Engel	EUROCAE
Alexander	Engel	EUROCONTROL
Zhe	Fan	COMAC BASTRI
Christian	Fiore II	The MITRE Corporation
Roman	Fischer	Skyguide
John	Flores*	Federal Aviation Administration (FAA)
Joacy	Freitas*	ANAC-Brazil
Patricia	Fuilla-Weishaupt*	Airbus
Raoufou	Ganiou	Transport Canada
Eduardo	Garcia	CANSO
Marty	Gasiorowski	Worldwide Certification Services
Armelle	Gauthe	Airbus
Gilles	Gobbo	Airbus
Cesar	Gomez	Federal Aviation Administration (FAA)
Will	Gonzalez	Federal Aviation Administration (FAA)
Elena	Gromova	GOSNIIAS
Judicael	GROS-DESIRS	AIRBUS SAS
Edward	Hahn*	Air Line Pilots Association (ALPA)
Jerry	Hancock	Inmarsat
Christian	Haury	Safran Electronics & Defense
Brian	Hoffman	Air Line Pilots Association (ALPA)
Anne-Cecile	Kerbrat	Dassault Aviation
Varun	Khanna*	Federal Aviation Administration (FAA)

Andrew	Kornecki	Embry-Riddle Aeronautical University
Marcus	Labay	Federal Aviation Administration (FAA)
Christopher	Lacey	AIRBUS SAS
Kristof	Lamont	EUROCONTROL
Laurent	Leonardon	Collins Aerospace
Jerome	Lephay	Collins Aerospace
Qi	Li	Department of National Defence
Marc	Lord	Transport Canada
Cyril	Marchand	Thales Group
Philippe	Marquis*	Dassault Aviation
Andrew	McLaughlin	Honeywell International, Inc.
Peter	McNeely	Astronautics Corporation of America
Patrick	McTernen	American Airlines, Inc.
Kevin	Meier	Cessna Aircraft Company
Stephane	Miglio	Airbus
Dinkar	Mokadam	Association of Flight Attendants
Jean-Paul	Moreaux	European Aviation Safety Agency (EASA)
Cecile	Morlec	Airbus
Catherine	Morlet	European Space Agency
Joe	Morrissey	The MITRE Corporation
Patrick	Morrissey*	Collins Aerospace
Michal	Mrazek	Honeywell International
David	Munoz	Thales Group
Ravi	Nori*	Teledyne Control
Siobvan	Nyikos	The Boeing Company
Thomas	Obert	Airbus
Ted	Patmore*	Delta Air Lines, Inc.
Mark	Perini	Honeywell International, Inc.
Tom	Phan	Federal Aviation Administration (FAA)
Aaron	Renshaw	American Airlines, Inc.
Philippe	Robert	PMV Engineering
Lionel	Robin	SAFRAN
Marc	Ronell	Federal Aviation Administration (FAA)
Chuck	Royalty*	Aerospace Systems Cyber Security
Shohreh	Safarian	Federal Aviation Administration (FAA)

Romuald	Salgues	Airbus
Krishna	Sampigethaya	United Technologies Corporation
Michael	Schraub	DFS Deutsche Flugsicherung GmbH
Stefan	Schwindt*	GE Aviation Systems UK
Remzi	Seker	Embry-Riddle Aeronautical University
Rebecca	Selzer	United Airlines, Inc.
Michael	Severson	Bell Helicopter Textron, Inc
Charles	Sheehe	NASA
Matt	Shreeve	Helios - UK (EUROCAE Member)
Peter	Skaves	Federal Aviation Administration (FAA)
Brittany	Skelton*	The Boeing Company
Kristopher	Smith	Triumph Group
Stephen	Sterling	Department of National Defence of Canada
Seth	Stewart	ENSCO Avionics Inc.
Hugo	Teso	Emirates
Christian	Tettamanti	ACI EUROPE
Casey	Theisen	United Airlines, Inc.
Lirong	Tian	Aeronautics Computing Technique Research Institute (ACTRI)
Timothy	Tinney	Saab Group
Christophe	TRAVERS	DASSAULT AVIATION
Mitchell	Trope	Garmin Ltd.
Isidore	Venetos	Federal Aviation Administration (FAA)
Herman	Verhoef	IATA
Brian	Verna	Federal Aviation Administration (FAA)
Ivan	Vincze	HungaroControl
Anna	von Groote	EUROCAE
Tong	Vu	Federal Aviation Administration (FAA)
Mohammed	Waheed	Aviage Systems
Adrian	Waller	Thales Group
Jeffrey Jeng Hang	Wang	FLYING WHALES
Philip	Watson*	Panasonic Avionics Corporation
Stephen	Williams	NATS
Matt	Winslow	Gulfstream Aerospace Corporation
Marcie	Wise	Delta Air Lines, Inc.

Thomas	Wittmann	ESG Elektroniksystem- und Logistik-GmbH
Cameron	Wright	Southwest Airlines Co
Dongsong	Zeng	The MITRE Corporation

APPENDIX B

AIRPLANE INFORMATION SECURITY PLAN (AISP)

(informative)

The material introduced in this appendix is for information only and does not constitute a mandatory part of this document.

Purpose

The purpose of this appendix is to provide an example of an Aircraft Information Security Program (AISP) template to help operators write their AISPs. In the US, this is called an Airplane Network Security Program (ANSP). For the purposes of a harmonized DO- 355A / ED-204A, it is called the Airplane Information Security Plan (AISP) so as not to cause confusion with the meaning of the ANSP acronym in Europe, which is Air Navigation Service Provider. The operator can continue to call it an ANSP or whatever they wish so long as the plan contains all the necessary information to support continued airworthiness security.

An AISP is needed prior to aircraft delivery. The AISP is maintained until the aircraft is transferred to another operator or retired. The AISP should be authorized prior to taking delivery of the aircraft. This maintains the security coverage that starts at airplane delivery and ends in the storage facility.

The connected airplane models incorporate an internet protocol network to integrate several airplane systems. These airplanes are required to meet the requirements of the Aircraft Security Operator Guidance (ASOG), which is described in DO-326A / ED-202A and addresses the Special Conditions for airplane network security. The ASOG requires that operators should develop and adhere to an Airplane Cybersecurity Plan. Several operators have been challenged in trying to interpret the ASOG into a plan and objectives that will be reviewed and authorized by the regulators. The ASOG and AISP are highly recommended by the OEM to maintain a secure airplane network and the supporting ground systems. To assist operators in developing their submittals to their local Civil Aviation Authorities (CAA), this AISP Operator Template provides suggested guidance both in format and in the minimum set of topics to comprehensively address secure ground data distribution and airplane network.

References

- FAA AC 119-1 - Operational Authorization of Aircraft Network Security Program (ANSP)
- DO-355A/ED-204A, “Information Security Guidance for Continuing Airworthiness” (this document)
- DO-356A/ED-203A, “Airworthiness Security Methods and Considerations”
- DO-326A/ED-202A, “Airworthiness Security Process Specification”
- ISEM, “Guidance on Information Security Event Management”
- Aircraft Security Operator Guidance (ASOG)

AISP Document Template – Proposed Table of Contents

1. Introduction
    a. Overview
    b. Purpose
    c. User Audience
    d. Responsibility & Authority

    Additional recommendations for Responsibility & Authority:

    - *Identify who has overall responsibility, i.e. Vice President of Maintenance, Engineering, Technical Services*
    - *Who has responsibility for the quality of the AISP, including who has the authority to change the plan/program, change board reviews and its members, etc.*

- *Airline/operator focal who serves as the Data Security Manager (DSM), authority to establish the policies, procedures and processes, including who in the airline will receive notifications and alerts from the OEM*
- *Who is responsible for the Loadable Software Airplane Part Librarian (LSAPL)*
- *Who will notify the local Civil Aviation Authority (CAA) inspector of changes to the AISP and within what specified number of days. Note: the FAA requires 30 days notification.*
- *Responsibility flow chart and organization chart*

e. AISP Revisions, Bulletins, and User Feedback

Additional recommendations for AISP Revisions, Bulletins, and User Feedback:

- *Include requests or recommendations concerning changes, additions, or deletions to this document, submitted using the airline document change processes*

2. Security Environment Description

Additional recommendations for Security Environment Description:

- *Risk Assessment*
- *Activity monitoring*
- *Vulnerability scanning to include validation of new software prior to airplane load*
- *Ground system validation to include application and security updates*
- *Periodic AISP validation with operator and CAA to ensure network security integrity (interval negotiated with CAA)*
- *General description of AISP “footprint”, covering all areas from software acceptance to software loading on the airplane target system*

3. Network Security Requirements

Requirements are usually tied to regulatory/certification, in this case the log retention.

a. Network Security Logs

i. Log Retrieval

ii. Log Analysis

iii. Log Event Management

iv. Interfaces

Additional recommendations for Network Security Logs:

- *Develop a security log management policy*
- *Establish procedures for secure transfer/storage of security log files*
- *Identify airplane references for log retrieval instructions*
- *How long log files will be retained per agreement with local CAA*
- *Establish audit policies and procedures*
- *Establish log file analysis processes with known baseline norms*

4. Network Security Recommendations

Recommendations are industry standards or best practices.

a. Control of Mobile Device Access and Utilization

Additional recommendations for Control of Mobile Device Access and Utilization:

- *Who is authorized to use mobile devices*
- *What is the training criteria for user*
- *How are devices secured*

- *Provide misuse guidance-policy*
- *Include lost device procedures*
- *Establish a password policy that meets or exceeds industry recommendations*
- *Establish audit policies and procedures*

b. Control of Portable Maintenance Devices (PMD), Removable Media, and Ground Support Equipment (GSE)

Additional recommendations for PMD, Removable Media, and GSE:

- *Who is authorized to use maintenance devices*
- *What is the training criteria for user*
- *How are devices secured to include storage locations*
- *Provide instructions on how devices are updated, security patches, etc.*
- *Provide misuse guidance-policy*
- *Limit PMD/GSE use to aircraft maintenance only, i.e. do not allow personal use*
- *Strictly prohibit the use of personal removable media*
- *Include lost device procedures*
- *Establish a password policy that meets or exceeds industry recommendations*
- *Establish audit policies and procedures*

c. Control of Access to Airport Off-board Network Services (Wired and Wireless)

Additional recommendations for Control of Access to Airport Off-board Network Services:

- *Who is authorized to use wired and wireless services*
- *List airport service provider for wireless and reference to contractual agreement*
  - *Adherence to the AISP*
  - *Including maintenance*
  - *Level of service agreement - speed, bandwidth, % reliability, etc.*
  - *List providers' security protection interfaces*
  - *Security certificates to be managed and be compatible with operator's ground system*
  - *PKI certificate renewal dates and intervals - how often*
- *List MRO maintenance provider using wireless services*
- *What is the training criteria for end user*
- *How are interfaces secured*
- *Establish audit policies and procedures*

d. Control of Access to Loadable Software Airplane Parts (LSAP) Librarian Resources and Ground Servers

Additional recommendations for Control of Access to LSAP Librarian Resources and Ground Servers:

- *Who is authorized to use LSAP services*
- *List operator third party IT services as required and reference contractual agreement*
  - *Include maintenance*
  - *Level of service agreement - speed, bandwidth, % reliability,*

etc.

  - *List providers' security protection interfaces*
  - *Security certificates to be managed and be compatible with operator's ground system*
- *What is the training criteria for end users*
- *How are interfaces secured*
- *Add LSAP flow diagram and matrices to skills or functional departments- engineering, quality, maintenance, etc.*
- *Establish audit policies and procedures*

e. Creating Secure Parts Management Processes

Additional recommendations for Creating Secure Parts Management Processes:

- *Who is authorized to create, maintain and issue keys management services*
- *If the operator creates new keys, list the procedures*
- *List operator third party Key Provider services as required and reference contractual agreement*
  - *Including maintenance*
  - *Level of service agreement for keys processing*
  - *List providers' security protection interfaces*
  - *Security certificates to be managed and be compatible with operator's ground system*
- *What is the training criteria for key providers and key end users*
  - *Matrices to skills or functional departments - engineering, quality, maintenance, etc.*
- *What actions should be taken when keys expire or compromised*
  - *Add key processing and renewal flow diagram.*
- *Establish audit policies and procedures*

f. Removal of Secure Parts

Additional recommendations for removal of secure parts form aircraft or components prior to the operator losing operational control:

- *Long term storage*
- *Disposal*

g. Control of Physical Access to Airplane

Additional recommendations for Control of Physical Access to Airplane:

- *Who is authorized to gain access to the airplane's data access ports (that are not accessible to passengers during a flight due to location, physical security, etc.)*
- *Establish and list secure zones on the aircraft*
- *List operator third party maintenance services as required to support data distribution and reference contractual agreement*
  - *Including maintenance*
  - *Level of service agreement*
  - *List providers' training*
- *Establish audit policies and procedures*

h. Control of Aircraft Conformity to Type Design

Additional recommendations for Control of Aircraft Conformity to Type Design (to cover both software and hardware conformity to design):

- *Who is authorized to create, maintain and issue aircraft conformity changes*

- *Establish a scheduled and on-demand software configuration check (see AC 43-216 for more information)*
- *Establish audit policies and procedures*

Airplane Testing Disclaimer: Invasive testing such as that requiring code injection or system tampering on a certified and conformed, delivered airplane risks the airplanes Airworthiness Certification. This could result in non-conformance to the type design of the airplane and lead to aircraft grounding.

i. Ground Safety Procedures

Additional recommendations for Ground Safety Procedures:

- *Include the OEM safety reference instructions and procedures*
- *Include on the job training (OJT) and recurrent training*
- *Airline's safety guidance and policy references*

5. Provisions for Parts Pooling and Borrowing

Additional recommendations for Parts Pooling and Borrowing:

- *Who is authorized to provide parts pooling authority*
- *Does the operator practice pool or borrow software? List airline process, include differences in operation locations as applicable*
- *List operator third party maintenance services as required to support data distribution and reference contractual agreement*
  - *Including maintenance*
  - *List parts pooling locations and security*
  - *Level of service agreement*
  - *List providers' training*
- *Does the operator prohibit pooling or borrowing of certain parts (specified by AISP)?*
  - *If so, what are those parts?*
- *Is there a procedure to remove security logs for parts being pulled or borrowed to prevent transfer to another airplane?*
- *Establish audit policies and procedures*

6. Procedures for Part Exchanges within Fleet

Additional recommendations for Procedures for Part Exchanges within Fleet:

- *Who is authorized to provide parts exchange authority*
- *List operator third party maintenance services as required to support data distribution and reference contractual agreement*
  - *Including maintenance*
  - *List parts exchange services locations and security*
  - *Level of service agreement*
- *Is there a procedure to remove security logs for parts being pulled or borrowed to prevent transfer to another airplane?*
- *Establish audit policies and procedures*

7. Security Event Recognition and Response

Please Refer to ISEM Guidance on Information Security Event Management and ensure AISP aligns with industry guidance.

8. Considerations for Program Improvement

Additional recommendations for Considerations for Program Improvement:

- *User feedback and change board reviews*
- *Who will evaluate the digital data user report/issue*
- *What is the resolution process and who notifies the effective airline department for change consideration, i.e. document, procedures,*

training, updates

- *Annual AISP reviews and recommendations from lessons learned*

9. Training and Qualifications

   Additional recommendations for Training and Qualifications:

   - *Baseline user training established and concurred by CAA inspector*
   - *Periodic digital data users' OJT, recurrent training, annual reviews/renewals*
   - *Annual processes' reviews*
   - *Establish training for users of LSAPs - creators, engineering, quality and maintenance (MRO) technicians*
   - *Verification and concurrence with local CAA for recommended guidance*

10. MRO and 3rd Party Maintenance

    Additional recommendations for MRO and 3rd Party Maintenance:

    - *Statement that MRO support complies to AISP*
    - *List MRO authority and impacted focals*
    - *Operator periodic reviews with MRO providers*
    - *List any MRO staff required training and qualifications*
    - *MRO to provide evidence of completed training*
    - *Include MRO LSAP distribution and security*
    - *Specify only approved device use*
    - *Limit or prohibit third party acceptance or distribution of LSAP beyond device to aircraft connectivity*

11. Acronyms

12. Reference Documents

    a. Airline Documents

    b. Regulatory references (FAA, EASA, etc.)

    c. OEM Documents

    d. Industry Security Guidance

13. Aircraft Security Operator Guidance (ASOG) Checklist

    Please refer to the specific requirements and recommendations from the applicable Aircraft Security Operator Guidance (ASOG) from OEM to form the checklist.

APPENDIX C

GLOSSARY OF TERMS

Term	Definition
Activity	Tasks that provide a means of meeting the objectives.
Airborne Software	Airborne software encompasses Aircraft Controlled Software (ACS, equivalent to Field Loadable Software (FLS)), Hardware Controlled Software (HCS) and Firmware (configuration of FPGAs (Field Programmable Gate Arrays) and other complex electronic hardware)
Aircraft	An aircraft or “aeroplane” means an engine-driven fixed-wing aircraft heavier than air that is supported in flight by the dynamic reaction of the air against its wings" (from Regulation (EU) No 965/2012)
Aircraft component	An aircraft component is a component approved for installation on a type-certificated aircraft.
Aircraft Information Security Center	The Aircraft Information Security Center should act as the operator’s point of contact for aircraft information security events from within and outside the operator’s organization.
Aircraft Type Certification	Design approval of an aircraft establishing that it ensures compliance with the applicable airworthiness requirements.
Airworthiness	The condition of an item (aircraft, aircraft system, or part) in which that item operates in a safe manner to accomplish its intended function. [Source: ARP 4754A]
Airworthiness Security	The protection of the airworthiness of an aircraft from the information security threat: harm due to human action (intentional or unintentional) using access, use, disclosure, disruption, modification, or destruction of data and/or data interfaces. This also includes the consequences of malware and forged data and of access of other systems to aircraft systems.
Assumptions	Statements, principles, and/or premises offered without proof. [Source: ARP 4754A]
Attack	An assault on system that derives from an act that is an attempt to violate the security policy of a system. This includes intentional and unintentional acts.
Certificate Revocation List (CRL)	A computer file that contains the list of all digital certificates that is revoked and thus is no longer valid and reliable.
Certificate Authority (CA)	A component of the Public Key Infrastructure. The CA is responsible for issuing and verifying digital certificates. [Source: GSA Government Smart Card Handbook]
Continued Airworthiness	All the actions associated with the upkeep of a type design and the associated approved data through life.
Continuing Airworthiness	All of the processes ensuring that, at any time in its operating life, the aircraft complies with the airworthiness requirements in force and is in a condition for safe operation.
Crate	Digital container for aircraft software parts and related digital products used for electronic distribution between aerospace business partners. [Source: ARINC 827]
Data Distribution	The ground based process of moving airborne software and data from a source location to a destination location and the process of storing software

	and data at each location. Examples of source and destination locations are software vaults, airborne software servers, Aircraft on-board mass storage, and OEM software distribution systems.
Data Loading	The process of moving airborne software and data from a storage source into the active executable memory of aircraft systems. Examples of storage sources are aircraft on-board mass storage, Portable Data Loader (PDL) mass storage or media, Aircraft Data Loader (ADL) mass storage or media, and software vault servers.
Defense in Depth	An architectural strategy in which more than one security measure is used such that a successful attack would require vulnerabilities in multiple security measures.
Design Approval Holder	A design approval holder is the holder of a type certificate, a Parts Manufacturer Approval or a Technical Standard Order authorization or the licensee of a Type Certificate. ***NOTE:*** *References to a type certificate includes supplemental type certificates unless noted otherwise.* All design approval holders must: • Report failures, malfunctions, and defects • Make Instruction for Continued Airworthiness (including changes) available to each aircraft, aircraft engine or propeller owner • Satisfy Additional Obligations for: Parts Manufacturer Approval Holder, Technical Standard Order Authorization Holders and Type Certificate Holders [Source: FAA]
Digital Certificate	The term digital certificate refers to the private key and the associated public key of the digital certificate. The sender's private key is used for signing and the receiver's private key for decrypting; the sender's public key is used to verify the signature and receiver's public key for encrypting.
Electronic Distribution of Software	Electronic airborne software distribution or Electronic Distribution of Software (EDS) is the process of electronically moving software and data from one location to another location, wired or wirelessly, without the use of portable electronic media such as magnetic disks, optical disks, or flash drives. See ARINC Report 827 for description of EDS.
External Agreement	Assumptions and requirements for the purpose of coordinating roles and responsibilities between dependent systems and external actors.
Field Loadable Software (FLS)	FAA 8110.49 defines Field Loadable Software as follows: Software that can be loaded without removal of the equipment from the installation. FLS can also refer to either executable code or data (see EUROCAE ED-12B / RTCA DO-178B). FLS might also include software loaded into a line replaceable unit at a repair station or shop. [Source: ARINC 667]
Ground Support Information System (GSIS)	Ground Support Information Systems (GSIS) are Ground Systems that are used to accomplish the process of Data Distribution and storage of Airborne Software and Data. Systems for creation and modification of UMS and UCS are also in the scope of Ground Support Information Systems
Ground Support Equipment (GSE)	Refers to Ground Support Equipment that digitally connects to the aircraft at any time during ground or maintenance operations
Hardware Controlled Software (HCS)	All airborne software which is configuration managed by the hardware part number of the hardware which contains the software is considered Hardware Controlled Software (HCS)
Information	Information is the (subjective) interpretation of data.

Information security	Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction. It is a general term that can be used regardless of the form the data may take (electronic, physical, etc.) [Source: Wikipedia]
Information Security Management System (ISMS)	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. ***NOTE:*** *The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.* [Source: ISO 27001]
Information Security Threat	A circumstance or event with the potential to affect the Aircraft due to human action (intentional or unintentional) resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or Information System interfaces. Note that this includes Malware and the effects of external systems on Dependent Systems, but does not include physical threats.
Instruction for Continued Airworthiness	Instructions for Continued Airworthiness are the instructions and information that are necessary for the continued airworthiness of the aircraft, engine, propeller, parts and appliances, which are required in accordance with the applicable Certification Basis or Standard to be developed and/or referenced by the Design Approval Holder. [Source: EASA]
Inter-company	Between different companies
Intra-company	Within one company
Media	Devices or material, which acts as a means of transferring or storage of software (e.g., programmable read-only memory, magnetic tapes or discs). [Source: ARINC 667]
Operational environment	The set of defined concepts of operations, regulations, plans, policies, and procedures of the external organizations and systems that interact with the dependent systems of the aircraft, together with any regulations and policies which apply internally to the aircraft systems themselves.
Operational Security Measures	Security measures that is applied during the operation of the aircraft
Operator	The operator is the organization that operates an aircraft or is responsible of the maintenance of the aircraft.
Security Event	A security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security relevant. [Source: ISO27000]
Security Incident	A single or a series of unwanted or unexpected information security events that could potentially affect aviation safety. [Source: adapted from ISO27000]
Security Measure	Used to mitigate or control a threat condition. Security measures may be features, functions or procedures, both on-board or off-board. Security measures can be technical, operational, or management. [Source: ED-202A / DO-326A]
Supplier Controlled Software	The supplier of this type of software is the TC/STC holder or the developer of the software. Changes to Supplier Controlled Software (SCS) require approval by the certification authority.

	[Source ARINC 667]
System Hardening	The process of securing a system by reducing its surface of vulnerability. Reducing available vectors of attack typically includes the removal of unnecessary software, unnecessary usernames or logins and the disabling or removal of unnecessary services.
Technical Vulnerability Management	Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities. This practice generally refers to software vulnerabilities in computing systems however it can also extend to organizational behavior and strategic decision-making processes. Refer also to ISO 27001 / 27002.
Trust Anchor	A Trust Anchor (also known variously as a Certificate Authority Certificate or a Root Certificate) is a certificate that is used as the basis for verifying the digital signature of a certificate, or for validating a chain of certificates. [Source: ATA Specification 42]
Trusted Area	Physical location where there is no threat against the asset (FLS, PDL, PMAT, etc.)
TSO	Technical Standard Order
User Certifiable Software (UCS)	When this software is modified, it should be reviewed and approved by the appropriate Airworthiness Certification Office. [Source: ARINC 667]
User Modifiable Software (UMS)	This is software that is intended for modification by the aircraft operator (airline) without review by the certification authorities, the airframe manufacturer, or the equipment vendor. A tool is usually provided so the software can only be modified within given boundaries. [Source: ARINC 667]
Vulnerability	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. [Source: ED-202A / DO-326A]
Whitelist (WL)	A whitelist is a computer file that lists all authorized digital certificates that have permission to access to a certain system or protocol. Any entity that is not included in the Whitelist has its access, to the system or protocol, denied.

APPENDIX D

ACRONYMS

Acronym	Definition
ACS	Aircraft Controlled Software
AISP	Aircraft Information Security Program
AISS	Aeronautical Information System Security
ALS	Airworthiness Limitation Section
AMM	Aircraft Maintenance Manual
ANSP	Aircraft Network Security Program
ATC	Air Traffic Control
ATE	Automated Test Equipment
CA	Certificate Authority
CASA	Civil Aviation Safety Authority of Australia
CBL	Certificate Blacklist
CBT	Computer Based Training
CLMT	COTS Laptop Maintenance Terminal
CMM	Component Maintenance Manual
COTS	Common Off-The-Shelf
CRL	Certificate Revocation List
DAH	Design Approval Holder
EASA	European Aviation Safety Agency
EDS	Electronic Distribution of Software
EIS	Entry Into Service
FAA	Federal Aviation Administration
FIM	Fault Isolation Manual
FLS	Field Loadable Software
GSE	Ground Support Equipment
GSIS	Ground Support Information System
HCS	Hardware Controlled Software
ICA	Instruction for Continued Airworthiness
IPC	Illustrated Parts Catalogue
ISEM	Information Security Event Management
ISMS	Information Security Management System
IT	Information Technology
MRBR	Maintenance Review Board Report
MRO	Maintenance, Repair and Overhaul
MSD	Mass Storage Device

OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
PDL	Portable Data Loader
PKI	Public Key Infrastructure
PMAT	Portable Maintenance Access Terminal
SARPS	Standards and Recommended Practices
SCS	Supplier Controlled Software
SeMS	Security Management System
SMS	Safety Management System
STC	Supplemental Type Certificate
TC	Type Certificate
TCCA	Transport Canada Civil Aviation
TSM	Trouble Shooting Manual
UCS	User Certifiable Software
UMS	User Modifiable Software
USB	Universal Serial Bus
WL	Whitelist

APPENDIX E

REFERENCES

NOTE: *The reader of this document should use the applicable revisions of the documents indicated below.*

Reference	Document
ARINC 645	Common Terminology and Functions for Software Distribution and Loading
ARINC 667	Guidance for the Management of Field Loadable Software
ARINC 811	Commercial Aircraft Information Security Concepts of Operation and Process Framework
ARINC 823	Datalink Security
ARINC 827	Electronic Distribution of Software By Crate (EDS Crate)
ARINC 835	Guidance for Security of Loadable Software Parts Using Digital Signatures.
ARINC 842	Guidance for Usage of Digital Certificates
EUROCAE ED-202A RTCA DO-326A	Airworthiness Security Process Specification
EUROCAE ED-XXX / RTCA DO-XXX	Guidance on Information Security Event Management (At the time of publication of DO-355A / ED-204A, DO-XXX / ED-XXX is under work) – ISEM
EU 748/2012	Commission Regulation (EU) No 748/2012 of 3 August 2012 laying down implementing rules for the airworthiness and environmental certification of aircraft and related products, parts and appliances, as well as for the certification of design and production organisations • 21.A.3A - Failures, malfunctions and defects • 21.A.61 - Instructions for Continued Airworthiness
EASA CS 25 and AMC 25	Certification Specifications and Acceptable Means of Compliance for Large Aeroplanes • Instructions for Continued Airworthiness
EC 2042/2003 M.A.202	Part M Part 147 Part 66
14 CFR 21	CERTIFICATION PROCEDURES FOR PRODUCTS AND ARTICLES • 21.3 - Reporting of failures, malfunctions, and defects • 21.50 - Instructions for continued airworthiness and manufacturer's maintenance manuals having airworthiness limitations sections.
14 CFR 25	AIRWORTHINESS STANDARDS: TRANSPORT CATEGORY AIRPLANES • 25.1529 – Instructions for Continued Airworthiness • Appendix H - Instructions for Continued Airworthiness

14 CFR Part 121	OPERATING REQUIREMENTS: DOMESTIC, FLAG, AND SUPPLEMENTAL OPERATIONS • 121.375 – Maintenance and preventive maintenance training program • 121.703 - Service Difficulty Reports
AC 21-45	Para. 5.B Commercial Parts
FAA Order 8900.1 Volume 3 Chapter 61	Flight Standards Information System (FSIMS) – General Technical Administration
CAR	CAR 521.368 Instructions for Continuing Airworthiness AWM Chapter 525.1529 Instructions for Continuing Airworthiness AWM Chapter 525.1529 Appendix H
ATA Spec 42	Aviation Industry Standards for Digital Information Security
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-86	Guide to Integrating Forensic Techniques into Incident Response
NIST SP 800-61	Computer Security Incident Handling Guide
ISO / IEC 27001:2013	Information technology – Security techniques – Information security management systems – Requirements
ISO / IEC 27005:2011	Information Security Risk Management
ISO / IEC 27035:2011	Information Security Incident Management
ISO / IEC 27037:2012	Guidelines for identification, collection, acquisition and preservation of digital evidence
CMU/SEI-2003-HB-001	Organizational Models for Computer Security Incident Response Teams (CSIRTs)
SAE ARP 5150	In-Service safety assessment of transport airplanes in commercial service
SAE ARP 5151	In-Service safety assessment of General Aviation Aircraft and Rotorcraft in commercial use

APPENDIX F

REVISION HISTORY - ED-204A

Major change summary:

- Reference to ED-203A/DO-356A
- Reference to underwriting ED-XXX/DO-XXX ISEM document
- Reuse terminology now used in companion standards (IUEI, incident, event, typology of security measures…)
- Add of an AISP example in Appendix B
- Update of applicable regulation when needed
- Chapter MMEL removed as already addressed through safety
- Add consideration of confidentiality when needed
- Consider the need for management of vulnerabilities in software tools
- Revision of Chapters x.3 and x.4 fully rewritten to be more objective oriented and completed with state of the art.
- Chapters x.2 updated to insert additional security measures (e.g. decommissioning of GSE, vulnerability management in software tools, GSE or GSIS, access control for GSIS, certificate revocation
- Chapter 8 simplified to make reference to upcoming ISEM document
- Chapter 9.1 Modified to be clearer and refer to existing regulation
- Chapter 10 Service providers and third parties are now part of risk assessment

IMPROVEMENT SUGGESTION FORM

Name: ______________________________ Company: ______________________________

Address: ____

City: ____________________________________ State, Province: ______________________

Postal Code, Country: ________________________ Date: _______________________________

Phone: __________________________________ Fax: _________________________________

Email: ____________________________________

Document : ED- / DO- ____________________ Sec: ______ Page: _____ Line: ________

[ ] Documentation error (Format, punctuation, spelling)
[ ] Content error
[ ] Enhancement or refinement

Rationale (Describe the error or justification for enhancement): ____________________________
____
____

Proposed change (Attach marked-up text or proposed rewrite): ______________________________
____
____
____

Please provide any general comments for improvement of this document: ___________________
____
____
____

Return completed form to:

EUROCAE
Attention: Secretariat General
9 – 23 rue Paul Lafargue
93200 Saint-Denis
France
Email: eurocae@eurocae.net