FIJI AERONAUTICAL INFORMATION CIRCULAR

Civil Aviation Authority of Fiji
Private Bag (NAP0354), Nadi Airport
Republic of Fiji
Tel: (679) 6721 555;   Fax (679) 6721 500
Website: www.caaf.org.fj

AIC 15/18
Effective
8 NOV 2018
OPS/ATC

AIRCRAFT NETWORK SECURITY PROGRAM (ANSP)

1. **GENERAL**: The Civil Aviation Authority of Fiji in exercise of its powers under the provisions of sections 146 (1) (2) (3) and (4) of the Fiji Air Navigation Regulations 1981, appropriately issues guidance in the provision of approving Aircraft Network Security Program (ANSP)

2. **PURPOSE**: The purpose of this AIC is to provide guidance to the operator for managing the security of its aircraft network systems.

3. **APPLICABILITY**: This AIC applies to Fiji AOC holders who operate any of the following:-

- Boeing aircraft equipped with an On-board Network System (ONS) or Core Network, or
- Airbus aircraft equipped with a Network Server System (NSS).

4. **REFERENCES**: The following materials were referred to for the development of this AIC:-

- D615Z052-01 – Ground Network Security Guidelines Rev B; and
- New Op Spec D301
- D615Z008-04 - ANSOG Rev C, Boeing.

5. INTRODUCTION.

5.1 Previously, aircraft used aviation (ARINC 429/ARINC 629) or military (MIL-STD-1553) standard data buses to connect the flight avionics systems. Transmission Control Protocols (TCP) and/or Internet Protocols (IP) (TCP/IP) for passenger information and in-flight entertainment systems were physically and logically isolated from the critical flight avionics system.

5.2 New aircraft designs also use TCP/IP technology for the avionics systems (E-enabled aircraft), connecting both flight deck and cabin domains in a manner that virtually makes the aircraft an airborne interconnected network domain server. The architecture of this aircraft airborne network allows connectivity to external systems and networks, such as wireless airline operations and maintenance systems, satellite communications (SATCOM), email, the World

Wide Web, etc. The major benefit of TCP/IP is the ability to move data to and from the aircraft without the use of standard storage media.

5.3 Ground servers (airport gatelink network) connected wirelessly to the aircraft network, delivers software and also downloads data to/from the aircraft. This has resulted in the introduction of new vulnerabilities that may open access to on-board aircraft systems and impede their operations, thus creating safety and airline business concerns.

5.4 During the software distribution from the suppliers/vendors, hackers can also attempt to manipulate and corrupt the critical software meant for updating the aircraft avionics. The main safety threat is that intentional manipulation of genuine software or injection of fake software by well-informed hackers could go undetected.

5.5 Late detection of software manipulation, tampering with the aircraft administrative messages (i.e. upload commands, inventory requests and related responses) may lead, for instance, to false alarms, and general denial of services. Attacks on software distribution can all create unwarranted delays to flights and compromise safety.

5.6 In view of all of the above, the transmission of critical data necessitates the need for an Aircraft Network Security Program (ANSP) to ensure proper control during software handling/distribution and network security on-board the aircraft.

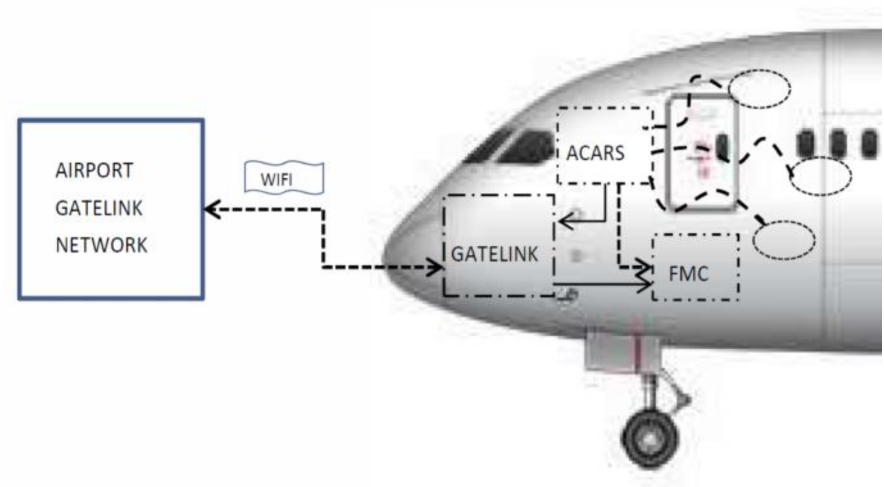

Figure 1.0 Airport Gatelink Network

5.7 The ANSP starts from the point whereby the software vendor/supplier transmit the software electronically (via internet) to the operator and from the operator through the wireless network or maintenance laptop to the aircraft and the execution by an approved person on the aircraft to load the software. Any changes made to the software configuration on the aircraft are treated with the same airworthiness intent as physical parts and will require the issue of a Certificate of Release to Service.

6. THREATS TO AIRCRAFT NETWORK SECURITY ARCHITECTURE.

6.1 On-board wired and wireless devices may have access to the aircraft network system to reprogram flight critical avionics components and may result in cyber security vulnerabilities from intentional or unintentional corruption of data and/or systems critical to the safety and continued airworthiness of the aircraft.

6.2 Threats also exist at access point of transmission through internet between software vendor/supplier to operator or its contractor and at points when the software is transmitted from the operator (airport gate-link) to the aircraft.

6.3 The ANSP shall be designed to protect the usability, reliability, integrity and safety of the network and data. Effective aircraft network security, targets a variety of threats and stops them from entering or spreading on the aircraft network which are associated with airworthiness.

6.4 Network security threats today are spread over the Internet. The most common include:-

- Hacker attacks
- Viruses, worms, and Trojan horses
- Denial of service attacks
- Data interception and theft
- Identity theft

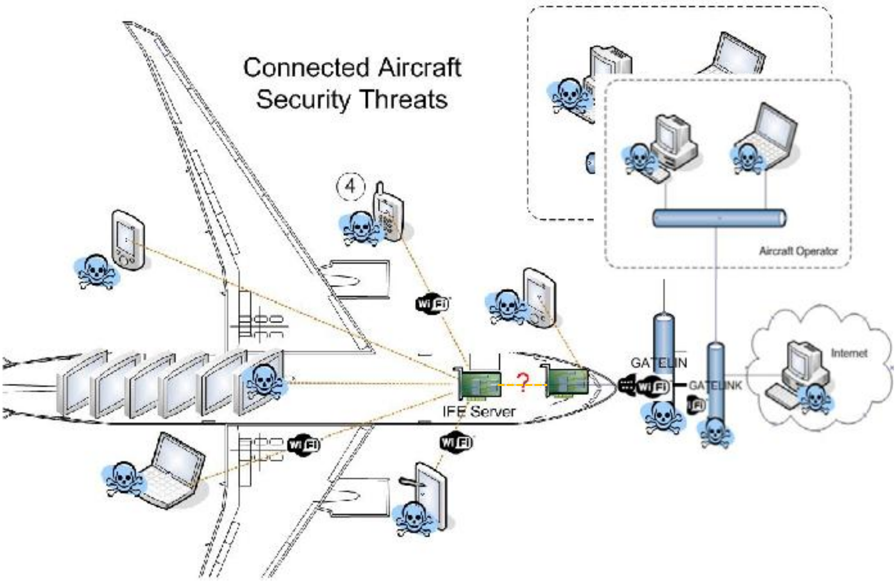

Figure 2.0 Connected Aircraft Security Threats

6.5 A successful attack can have adverse effects on the aircraft and its occupants. Threats can cause a wide variety of failures.

General Threat Identifiers	Aircraft Data Network Threats	Example of operational impact
Failure	**Safe state of the aircraft system could be compromised in the event of a security penetration**	**Access to the flight controls by unauthorised individuals affecting safety**
Denial	**Aircraft system resources exhausted due to denial of service attack, system error, malicious actions**	**Critical services disrupted by system overload or traffic jamming**
Access Control	**Individual other than an authorised user may gain access to the aircraft system via unauthorised controller, masquerade or spoofing system error or an attack for malicious purposes**	**Unauthorised Access**
Passive Attack	**Snooping or eavesdropping compromising security (misdirection). Flaws in security policies may lead to back door access**	**Unauthorised corruption or destruction of data causing unsafe flight conditions**

Table 1.0 Types of Failures

7. AIRCRAFT OPERATION THAT REQUIRES ANSP.

7.1 Aircraft with TCP/IP network systems are certificated through various means, such as Type Certificates (TC) and Supplemental Type Certificates (STC) that include Special Condition requirements (as with Boeing aircraft), or the Airworthiness Limitation Section (ALS) of the instructions for continued airworthiness (as with Airbus).

7.2 The FAA requires that the Type Design Holder issue a Network Security Document to provide the aircraft operator with the information necessary to maintain his aircraft in compliance with the Special Conditions. The operator uses this document as the basis to construct his ANSP Document. Similarly, EASA requires its Type Design Holder to issue a Security Document to provide the operator with information to construct his ANSP Document. Whenever there is a revision to the Security Document, the operator's ANSP Document shall also be revised as soon as possible

7.3 The aircraft Type Certificate holder (e.g. Boeing/Airbus) will also provide instructions on how to maintain the aircraft on-board network system to ensure system integrity and security. The instructions can be found in the Aircraft Maintenance Manual, Fault Isolation Manual, Service Letters or Service Bulletins.

7.4 The operator is reminded to follow the instructions regarding aircraft network security as specified in the documentations issued by the Type Certificate holder and also the actions recommended in this Advisory Circular.

8. SOFTWARE DISTRIBUTION AND STORAGE.

8.1 The aircraft uses software to provide logic or control for various system operations and functions and are regularly updated. The software is commonly known as Loadable Software Aircraft Part (LSAP) and is considered as part the aircraft's configuration. The LSAPs for the aircraft are constantly being reviewed and upgraded by the aircraft avionics OEMs. Once new or upgraded version software is certified, it can be distributed to the operators for uploading onto the aircraft On-board Electronic Distribution System (OBEDS).

8.2 Physical media such as CDs and DVDs have been used for managing, handling and distributing of LSAP. Nowadays the distribution of LSAP may be over an online delivery medium, such as the internet, without the use of physical media and then validated at the receiver end. This is referred to as the Electronic Distribution of Software (EDS). As mentioned, threats exist at access points of transmission and needs to be mitigated.

8.3 A process of validating of Electronic Distribution of Software (EDS) crates with the authorised manufacturers is important. The operator shall verify the authenticity of the software. Aircraft configuration and software used for this purpose will require protection from data corruption which includes damage caused by unauthorised users, viruses or other malware. The operator shall follow instructions from authorised manufacturer and crates that are unable to be identified and verified shall be destroyed.

8.4 The diagram below shows the distribution of software from the vendor/supplier to the operator storage facility using physical media and EDS Process through the internet. The crated software can be loaded onto the aircraft wirelessly or via a maintenance laptop.

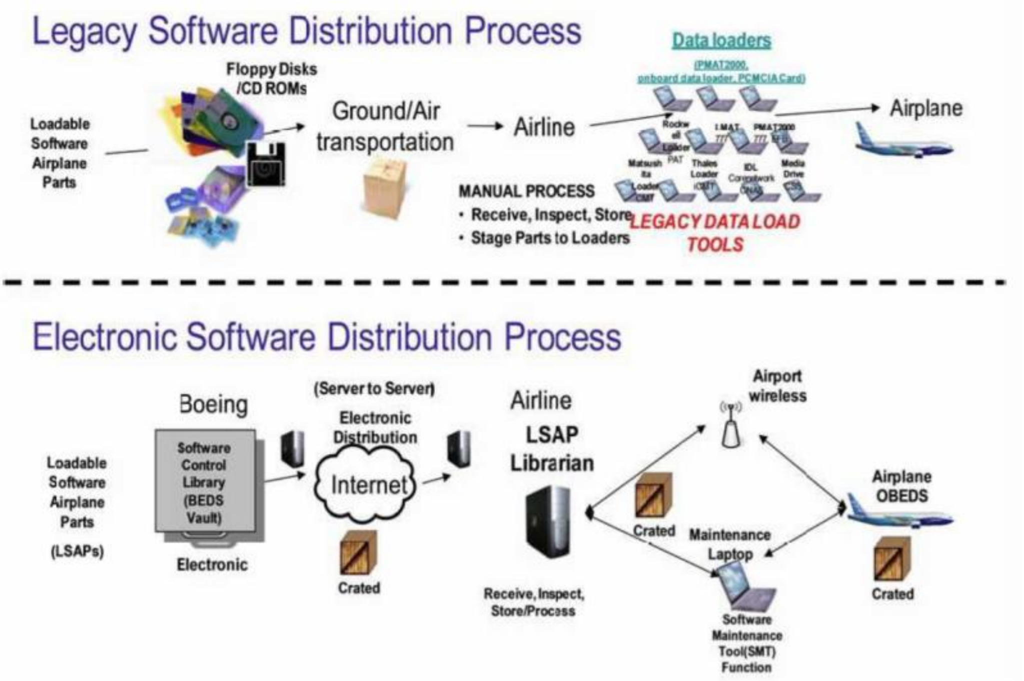

Figure 3.0 Electronic Distribution of Software

8.5 The following example of software distribution is typical of the process used to prepare and send software applications and other digital content.

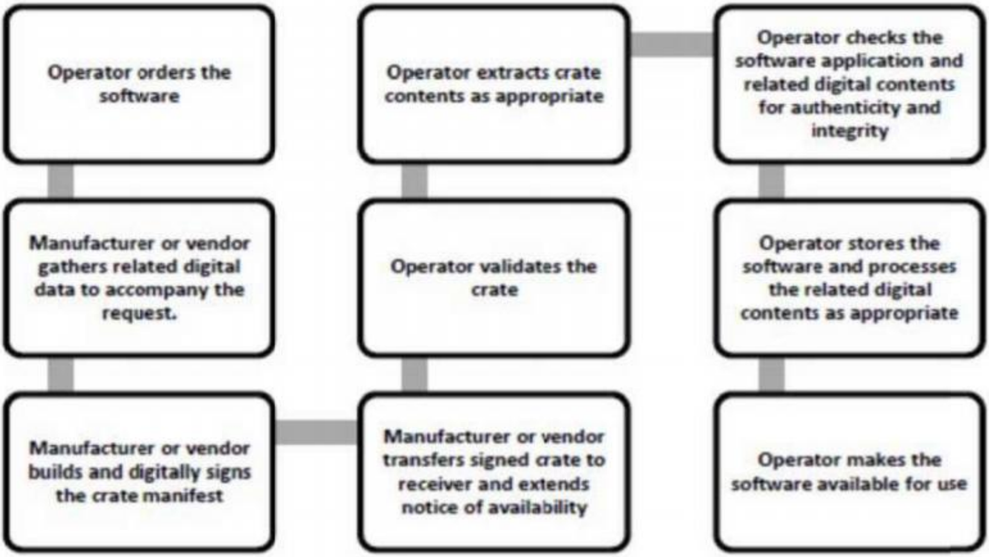
Operator orders the software
Manufacturer or vendor gathers related digital data to accompany the request.
Manufacturer or vendor builds and digitally signs the crate manifest
Manufacturer or vendor transfers signed crate to receiver and extends notice of availability
Operator validates the crate
Operator extracts crate contents as appropriate
Operator checks the software application and related digital contents for authenticity and integrity
Operator stores the software and processes the related digital contents as appropriate
Operator makes the software available for use

Fig 4.0 Digital Distribution Process

9. AIRCRAFT MAINTENANCE.

9.1 The operator is ultimately responsible for the ANSP and shall control every maintenance personnel (including contracted personnel) who may have access to or work on security sensitive systems.

9.2 The Maintenance Laptop is the primary maintenance system user interface with the aircraft that is used to update or change aircraft software configuration. Some Maintenance Laptop may make use of wireless connection to access aircraft software data. The access to and use of Maintenance Laptop shall therefore be tightly controlled. Steps shall be taken to make unauthorised use of wireless Maintenance Laptop difficult to accomplish and easy to detect. There shall be an effective means of controlling access to on-board maintenance functions to prevent unauthorised access to aircraft systems and data. The operator shall also put in place a process to deal with the loss or corruption of these devices.

9.3 The operator shall also have a process for producing an authorised software configuration for his aircraft and also verifying his aircraft meets this configuration. Maintenance personnel shall follow strictly the manuals/instructions from the aircraft manufacturer when implementing any changes to the aircraft configuration.

10. RISK ASSESSMENT.

10.1 Risk assessment is a fundamental component of risk management. The operator shall conduct risk assessment regularly to identify, estimate and prioritise risks to the aircraft network security programme. When weakness or deficiencies are discovered, mitigation measures shall be imposed and changes to operator's policy shall be made.

10.2 A security risk assessment is not complete until it includes the effects of all intended security controls and agreements with any third parties.

10.3 The operator shall consider wider ranges of possible threat scenarios to determine the potential harms associated with aircraft configuration and airworthiness. It is better to be over inclusive with risks than under-inclusive in conducting this analysis. Changes to company policy may be required to mitigate particular risks by reducing the likelihood that they will occur.

10.4 The operator shall regularly reassess the ANSP to ensure that the security requirements continue to be valid. Changes in technology or changes to the operator's business processes can possibly affect the validity of an ANSP. Any threats identified shall be reported to CAAF as required under Appendix Q of the Air Operator Certificate Requirements - *reference: AOCR, Appendix Q 2.1(b)(18) – Significant safety and security related events.*

11. RISKS MITIGATION MEASURES.

11.1 It is important that the operator establishes good practices over aircraft software and network security in a manner similar to IT security of an organisation. Failure to do so can compromise the airworthiness of the aircraft. Protection on wireless nodes must involve the use of authentication of users and data encryption. An encryption process transforms intelligible data, called plaintext, into an unintelligible form, called cipher text by the use of key.

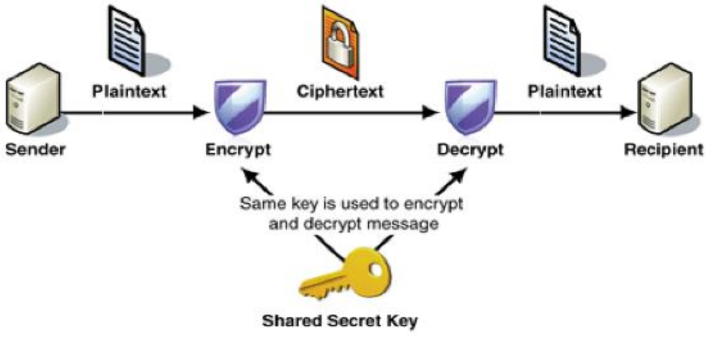

Fig 5.0 Encryption/Decryption Process

11.2 Decryption reverses this process, back to plaintext. If the cipher text changes in anyway, it will not decrypt correctly. Cryptography can therefore detect both intentional and unintentional modification.

11.3 A common technique used is called the Public Key Infrastructure (PKI). In order to decrypt a file, a key pair is required. The public key is widely distributed, whilst the recipient only has access to the private key. The public key verifies the signature process. Anyone can verify a correctly signed message using the public key. Decryption of an encrypted file utilises a private key. Security of the private key is important to keep the plaintext secret.

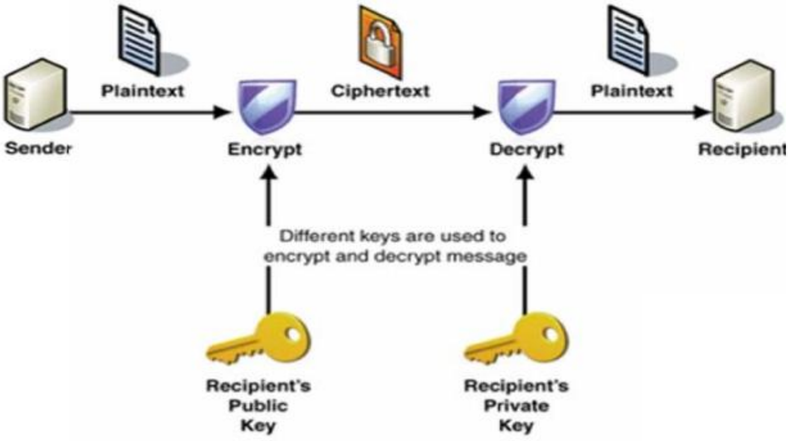

Fig 6.0 Public Key Encryption

11.4 A digital signature is used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged.

11.5 Mitigating measures shall be documented for assurance purposes. The operator shall classify and treat documentation on mitigating measures as confidential documents.

11.6 Any wireless service providers used for transfer of data shall be evaluated for security risks. These shall be documented in policies and procedures.

12. SECURITY LOGS.

12.1 The operator shall establish a log of authorised users who have access to change or amend the aircraft software configuration. The operator can monitor the ANSP with security logs. Computer security logs are audit logs that track any user authentication attempts. Security device logs are utilised to record any possible attacks to hardware. Log management is essential to ensure that computer security records are stored in sufficient detail for an appropriate period.

12.2 An attack of the system may have taken place when the log shows any of the following:

- Unusually heavy network traffic;
- Out of disk space or significantly reduced free disk space;
- Unusually high CPU usage;
- Creation of new user accounts;
- Attempted or actual use of administrator-level accounts;
- Locked-out accounts;
- Account in-use when an authorised user is not at work;
- Cleared log files;
- Full log files with unusually large number of events;
- Antivirus or other alerts;
- Disabled antivirus software and other security controls;
- Unexpected update changes;
- Machines connecting to outside IP addresses;
- Requests for information about the system (social engineering attempts);
- Unexpected changes in configuration settings; and
- Unexpected system shutdowns.

13. AIRCRAFT SECURITY LOGS.

13.1 An aircraft security log shall be maintained for each aircraft. The operator shall specify in his ANSP the frequency, methods of storage, retrieval and analysis of aircraft security logs. The aircraft security log is to be analysed for anomalies to understand normal system behaviour and identify security risks. It is beneficial to create duplicate log files, one file for immediate analysis and one for unaltered history.

13.2 Automated downloading of the aircraft security log files are not considered a maintenance task unless specified by the aircraft manufacturer.

14. PASSWORD CONTROL

14.1 Password control is considered the most simple and common form of user authentication. Password vulnerabilities can be reduced by changing passwords periodically and using an active password checker that prohibits weak, recently used, or commonly used passwords.

14.2 The operator shall keep private and public keys as secure as possible. A process for loss of password shall be addressed. In addition, a process is also required for expired or invalid digital signatures and certificates.

15. CRITICAL AREAS OF THE AIRCRAFT.

15.1 The flight deck, aircraft Electrical & Electronic Bays are critical areas of aircraft whereby equipment such as the wired Maintenance Laptop and automated test equipment interfaces with the aircraft avionics are located. These areas shall be restricted to authorised personnel only.

15.2 The operator shall ensure that unauthorised physical access to Cabin Attendant Stations/Panels is prevented, particularly when passengers are moving about the cabin.

16. AIRCRAFT NETWORK ADMINISTRATOR.

16.1 The operator shall appoint an administrator to be responsible for the security of aircraft information network. The role of such an aircraft network administrator is similar in requirement to an IT network security manager.

16.2 The aircraft network administrator shall be responsible for:-

- Managing any lost or stolen Ground Support Equipment (GSE) devices that are required for changing aircraft software configuration.
- Creating and controlling authorised user accounts.
- Decommissioning equipment or parts in a way that no data is recoverable from them.
- Providing logs, reports or other data to CAAF as required.
- Maintaining a password management programme for users.
- Maintaining records for equipment usage.
- Restricting any services, protocols, connections or nodes that are not required.
- Controlling access and utilisation for associated hardware required for aircraft network security programme.
- Quarantining any crates or files that contain invalid digital signatures, until there is a way of verifying the contents are authorised. Any invalidated crates shall be deleted.
- Controlling of any cryptographic keys used in aircraft network security programme.
- Controlling of any aircraft network security programme certificate expiration dates.
- Identifying and obtaining aircraft software applications required for maintenance or modification of the aircraft configuration.
- Verifying software applications and identifying any issues with associated hardware used for their installation.
- Ensuring suitable staging of software parts that will change aircraft configuration in a secure area, prior to installation on aircraft by appropriately licensed maintenance engineers.
- Retaining and monitoring aircraft network security programme logs.

- Retaining any changes to the aircraft configuration
- Keeping track of any changes required by the authorised manufacturer’s software security processes.
- Updating digital signatures if required for aircraft network security programme.
- Monitoring any expiration of digital signatures.
- Eliminating any viruses or other malware that could affect the aircraft and/or systems required for the aircraft configuration.

17. TRAINING.

17.1 Training for the aircraft network administrator shall be provided so as to enable him to perform his role more efficiently. The scope of the training on the aircraft network security programme shall be consistent with the requirements of the aircraft manufacturer

17.2 Authorised personnel shall be trained to understand good security practices and also the ability to troubleshoot security related events. All personnel involved in ANSP shall be familiar with the procedures defined in the ANSP.

18. USE OF CHECKLIST.

18.1 The operator shall make use of appropriate checklists provided by the aircraft manufacturer in implementing a management process for his aircraft network security program.