Civil Aviation Safety Authority
of Papua New Guinea

# Advisory Circular

# AC140-04

## Introduction and Certification of New Security Technologies

**Initial Issue**

**07 May 2025**

### GENERAL

Civil Aviation Safety Authority of Papua New Guinea Advisory Circulars (AC) contain information about standards, practices and procedures that the Director has found to be an Acceptable Means of Compliance (AMC) with the associated rule.

An AMC is not intended to be the only means of compliance with a rule, and consideration will be given to other methods of compliance that may be presented to the Director. When new standards, practices or procedures are found to be acceptable, they will be added to the appropriate Advisory Circular.

### PURPOSE

The purpose of this Advisory Circular (AC) is to provide guidance to aviation security service providers, aerodrome operators, and other relevant stakeholders on the introduction, evaluation, and certification of new security screening technologies within Papua New Guinea's civil aviation system. This AC supports compliance with PNG Civil Aviation Rule Part 140 and aligns with international best practices, including ICAO Doc 8973 and ICAO Doc 10047.

### RELATED CAR

This Advisory Circular relates to Rule 140.55 and Appendices A.4 and A.26 of PNG Civil Aviation Rules Part 140, which require the establishment of operational procedures and the use of approved screening methods and equipment. It also draws on the Director's authority under these provisions to approve methodologies and performance standards for security screening technologies. This AC supplements the regulatory framework by providing structured guidance for the evaluation, approval, and integration of new or emerging security technologies into operational environments, ensuring alignment with national and international aviation security standards.

### CHANGE NOTICE

This Advisory Circular (AC140-04) is the initial issue, introducing the first version of Introduction and Certification of New Security Technologies.

# TABLE OF CONTENTS

# 1. INTRODUCTION

## 1.1. Overview

This Advisory Circular (AC) provides guidance material and an Acceptable Means of Compliance (AMC) to assist airport operators and aviation security service providers in meeting the requirements of PNG Civil Aviation Rule (CAR) Part 140—specifically relating to the introduction, evaluation, and certification of new aviation security technologies.

The purpose of this AC is threefold:

- To ensure the consistent, risk-informed adoption of emerging security technologies in line with ICAO Standards and Recommended Practices (SARPs);
- To outline a structured and transparent process for proposing, testing, and integrating new technologies into aviation security operations;
- To define CASA PNG's expectations for safety, performance verification, operational suitability, and ongoing oversight of certified security technologies.

This AC supports innovation while safeguarding national aviation security objectives and is intended to provide clear procedures for both operators and service providers introducing new technologies into the PNG aviation system.

## 1.2. Scope

1.2.1 This AC applies to:

(a) Certified aviation security service organisations (ASSOs);

(b) Aerodrome operators and airport authorities;

(c) Security contractors and sub-contractors operating under CAR Part 140;

(d) Entities responsible for deploying, managing, or operating security technology for regulated security functions.

1.2.2 By adhering to the guidelines and procedures outlined in this AC, stakeholders can ensure that new security technologies are effectively integrated into the aviation security framework, enhancing overall security while maintaining compliance with regulatory requirements.

# 2. REGULATORY FRAMEWORK AND KEY DEFINITIONS

## 2.1 Overview of Relevant Regulations

2.1.1 This AC supports compliance with:

(a) CAR 140.9 – Certification application requirements for ASSOs;

(b) CAR 140.51–140.57 – Security programme, training, quality control, and recordkeeping;

(c) CAR 140.55 – Training requirements

(d) CAR 140.57 – Recordkeeping requirements

(e) CAR 140.59 – Incident reporting and coordination;

(f) CAR 140.61 – Requirements for security equipment and technology;

(g) CAR 140.63 – Procedures for the introduction and certification of new security technologies.

## 2.2 Compliance Requirements

2.2.1 Certified security service organisations must ensure all equipment and processes used in delivering aviation security services meet performance and reliability standards as outlined in PNG CAR Part 140. The use of unverified or uncertified technologies can undermine national aviation security objectives.

## 2.3 Key Definitions

2.3.1 **Security Technology** - Any technical system, equipment, or software used to detect, prevent, respond to, or investigate acts of unlawful interference in civil aviation.

2.3.2 **Certification** - The formal approval granted by CASA PNG for the operational use of a specific security technology or equipment.

2.3.3 **Operational Evaluation** - A field test under real airport conditions to assess effectiveness, interoperability, and impact on airport operations.

2.3.4 **Qualified Equipment List (QEL)** - A list maintained by CASA PNG of approved security equipment that meets the required standards and specifications.

# 3. PLANNING, CERTIFICATION, AND APPROVAL

## 3.1 Planning and Justification for New Technologies

3.1.1 Operators must justify the acquisition or deployment of new security technologies through a security risk assessment (SRA) and/or based on operational demands. The justification should include:

(a) Threat-based rationale (e.g., evolving threats, insider risk);

(b) Capacity or performance improvements;

(c) Compliance with PNG CAR Part 140 changes;

(d) Lifecycle replacement of obsolete equipment.

## 3.2 Certification and Pre-Deployment Approval

3.2.1 Before deploying a new technology operationally, the ASSO or airport operator must:

(a) Submit a Technology Certification Request to the Director, including:

(i) Product specifications and performance standards;

(ii) Certification reports from other compliant jurisdictions (e.g., ECAC, TSA);

(iii) Independent laboratory testing results (e.g., false alarm rate, detection sensitivity);

(iv) Intended deployment scope and use cases.

(b) The Director may:

(i) Approve equipment based on existing certifications from recognized authorities;

(ii) Require additional local trials or operational evaluations;

(iii) Assign a conditional approval pending full validation.

## 3.3 Operational Evaluation and Field Testing

3.3.1 Operators must conduct controlled field testing in coordination with CASA PNG to evaluate:

(a) Performance in operational conditions (e.g., detection under load);

(b) Compatibility with existing airport infrastructure;

(c) Staff proficiency and required training;

(d) Cybersecurity and data privacy risks;

(e) Reliability and maintenance requirements.

(f) CASA PNG may participate in these evaluations or require documentation of results prior to full approval.

# 4. INTEGRATION, TRAINING, AND MAINTENANCE

## 4.1 Integration with Security Programmes

4.1.1 The new technology must be:

(a) Incorporated into the Airport Security Programme (ASP) or AVSEC Manual;

(b) Reflected in updated SOPs, including:

(i) Equipment calibration and maintenance;

(ii) Alarm resolution and escalation;

(iii) Contingency planning for malfunctions;

(c) Supported by updated training plans for staff.

## 4.2 Training Requirements

4.2.1 Operators must ensure that:

(a) Personnel are trained in operation, troubleshooting, and response protocols;

(b) Training is conducted prior to equipment being put into operational use;

(c) Refresher training is included annually or when significant upgrades are made.

## 4.3 Maintenance, Calibration, and Recordkeeping

4.3.1 Operators must:

(a) Develop and follow a manufacturer-approved preventive maintenance schedule;

(b) Keep records of:

(i) Maintenance logs,

(ii) Calibration checks,

(iii) Software/firmware updates,

(iv) Faults or anomalies;

(c) Ensure service agreements are in place with qualified technicians.

(d) CASA PNG inspectors may review maintenance records during audits.

***Retention Period***: Minimum of 5 years per CAR 140.57.

# 5. CYBERSECURITY, INTEROPERABILITY, AND POST-IMPLEMENTATION REVIEW

## 5.1 Cybersecurity and Interoperability

5.1.1 New technologies that interface with networks or store sensitive data must adhere to stringent cybersecurity and interoperability standards to ensure the protection of sensitive information and seamless integration with existing systems. The following requirements must be met:

(a) **Cybersecurity Risk Assessments** - Conduct thorough cybersecurity risk assessments to identify potential vulnerabilities and threats. This includes evaluating the technology's resilience against cyber-attacks and unauthorized access.

(b) **Secure Configurations** - Implement secure configurations to safeguard the technology. This involves setting up firewalls, intrusion detection systems, and ensuring that default passwords are changed.

(c) **Encrypted Communications** - Ensure that all communications involving the technology are encrypted to protect data during transmission. Use industry-standard encryption protocols to secure data.

(d) **Access Control** - Establish robust access control mechanisms to restrict access to authorized personnel only. This includes using multi-factor authentication and role-based access controls.

(e) **Compatibility with Existing Systems** - Verify that the new technology is compatible with other airport security systems and does not degrade overall system performance. This includes ensuring interoperability with existing hardware and software.

## 5.2 Post-Implementation Review

5.2.1 After full deployment, the operator must conduct a comprehensive post-implementation review to assess the effectiveness and impact of the new technology. The review process includes the following steps:

(a) **Performance Assessment** - Evaluate the technology's performance in real-world conditions, including detection rates, false alarm rates, and overall reliability. This assessment should be conducted within six months of deployment.

(b) **Staff Feedback** - Gather feedback from staff who interact with the technology to identify any operational issues or areas for improvement. This includes assessing user satisfaction and ease of use.

(c) **False Alarm Rates** - Monitor and analyze false alarm rates to ensure the technology is accurately identifying threats without causing unnecessary disruptions.

(d) **Documentation and Reporting** - Submit detailed findings and any proposed adjustments to the Director. This includes providing documentation of the performance assessment, staff feedback, and any corrective actions taken.

By adhering to these requirements, operators can ensure that new security technologies are effectively integrated into the aviation security framework, enhancing overall security while maintaining compliance with regulatory standards.

# 6. ALTERNATIVE MEANS OF COMPLIANCE AND OVERSIGHT

## 6.1 Alternative Means of Compliance

6.1.1 Operators may propose alternatives to the prescribed methods if they achieve an equivalent or higher level of security. CASA PNG will assess these proposals on a case-by-case basis, ensuring that they meet the necessary security standards and provide adequate protection against threats. The process for proposing alternative means of compliance include:

(a) **Submission of Proposal** - Operators must submit a detailed proposal to the Director outlining the alternative methods and demonstrating how they meet or exceed the security requirements of PNG CAR Part 140.

(b) **Risk Assessment** - The proposal must include a comprehensive risk assessment, identifying potential vulnerabilities and mitigation strategies.

(c) **Supporting Documentation** - Operators must provide supporting documentation, including technical specifications, performance data, and any relevant certifications or approvals from recognized authorities.

(d) **Evaluation by CASA PNG** - CASA PNG will evaluate the proposal, considering factors such as effectiveness, reliability, and compatibility with existing security systems. This evaluation may involve consultations with experts and stakeholders.

(e) **Approval Process** - If the alternative methods are deemed acceptable, the Director will issue an approval, allowing the operator to implement the proposed methods. Conditional approvals may be granted pending further validation.

## 6.2 Oversight and Enforcement

6.2.1 CASA PNG retains the authority to oversee the implementation and operation of new security technologies, ensuring compliance with regulatory standards. The oversight and enforcement process includes:

(a) **Inspections and Audits** - CASA PNG will conduct regular inspections and audits of new technologies to verify compliance with PNG CAR Part 140. These inspections may include on-site visits, performance evaluations, and reviews of maintenance records.

(b) **Suspension or Revocation of Approval** - The Director may suspend or revoke the approval of a technology if it is found to be non-compliant with regulatory standards or if it poses a security risk. Reasons for suspension or revocation may include poor performance, failure to meet certification requirements, or significant security breaches.

(c) **Revalidation of Performance** - Following major incidents or failures, the Director may require revalidation of the technology's performance. This involves conducting additional tests and evaluations to ensure the technology remains effective and reliable.

(d) **Corrective Actions** - Operators must implement corrective actions to address any deficiencies identified during inspections or audits. CASA PNG will monitor the implementation of these actions to ensure compliance.

6.2.2 By adhering to these guidelines, operators can ensure that alternative means of compliance are

effectively integrated into the aviation security framework, enhancing overall security while maintaining regulatory compliance. CASA PNG's oversight and enforcement mechanisms provide a robust framework for monitoring and ensuring the effectiveness of new security technologies.