



### Airport Security Programme

Revision 1

08 May 2025

#### GENERAL

Civil Aviation Authority 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

This Advisory Circular provides methods, acceptable to the Director, for showing compliance with the Airport Security Programme Requirements of Part 107 and explanatory material to assist in showing compliance. Conformance with this AMC will facilitate acceptance of the entity's security programme.

#### RELATED CAR

This AC relates specifically to Civil Aviation Rule Part 107, which is required by Civil Aviation Rule Part 139.96

#### CHANGE NOTICE

The following are the Changes to the previous issue of this AC, consequently the change in effect; Inclusion of:

- (1) 107.51(a)(3)(i) – Additional guidance on the landside and airside boundary
- (2) 107.51(a)(3)(v) – Declared and enhanced security restricted areas are declared in accordance with a risk assessment.
- (3) 107.51(i) – Establish and implement procedures for review of the Airport Security Programme, including its amendments
- (4) 107.51(j) – Establish and implement procedures for distribution of Airport Security Programme.
- (5) 107.53(d)12 – Additional Requirements for cyber security
- (6) 107.53(d)(20) – Requirement for procedure for security controls including screening for merchandise and supply
- (7) 107.53(d)(21) - Requirement for procedure for unattended and suspicious object based on risk assessment

Published by Civil Aviation Authority of Papua New Guinea

## Table of Contents

<b>GENERAL .....</b>	<b>1</b>
<b>PURPOSE .....</b>	<b>1</b>
<b>RELATED CAR .....</b>	<b>1</b>
<b>CHANGE NOTICE .....</b>	<b>1</b>
<b>Subpart A — General .....</b>	<b>6</b>
107.1 Purpose .....	6
107.3 Definitions .....	6
<b>Subpart B — Airport Security Programme Requirements .....</b>	<b>6</b>
107.51 Airport Security Programme .....	6
107.51(a)(1): Airport Plan .....	6
107.51(a)(2) Airport Grid Map .....	6
107.51(a)(3) Map of the Airport .....	6
107.51(a)(4) Terminal Diagram Access Points .....	7
107.51(b)(1) Required Personnel .....	8
107.51(b)(2) Positions Responsible for Training of Personnel .....	8
107.51(b)(3): Identifying Key Airport Stakeholders .....	8
107.51(c): Current Contacts of Airport Stakeholders .....	8
107.51 d: Management of Security Sensitive Information .....	8
107.51(5): Airport Security Committee (ASC) .....	8
107.51(e)(1) Terms of Reference of ASC .....	8
107.51(e)(2) Composition of Members of ASC .....	9
107.51(e)(3) Frequency of ASC Meeting .....	9
107.51(e)(4) Management of Meeting Records .....	9
107.51(f): Details of Measures and Procedures .....	9
107.51(g) Contractual Provisions .....	9
107.51(h) Periodic Verification of Security Measures Outsourced to External Service Providers .....	10
107.51(i) periodic review of the Airport Security Programmes .....	10
107.51(j) Distribution of the Airport Security Programmes .....	10
107.53 Security requirements .....	10
107.53(a) Airport Security Programme .....	10
107.53(b): Safeguards for Preventing Inadvertent Unauthorized Access .....	10
107.53(c)(1): Physical barrier access points .....	10
107.53(c)(2) Control of any Duct, Drains or Tunnel .....	11
107.53(d) Construction and Height of Barrier .....	11
107.53(d)(1) Isolated Parking Position .....	14
107.53(d)(2) Emergency Lighting .....	15
107.53(d)(3) Potable Lighting for Designated Aircraft Parking Areas .....	16

107.53(d)(4)(i) Screening of International Passenger, Crew and their Baggage .....	16
107.53(d)(4)(ii) Sterile areas for International Passengers .....	16
107.53(d)(4)(iii) Mixing of screened and unscreened persons .....	16
107.53(d)(5) Enhanced Security Areas.....	17
107.53(d)(6) Security threat.....	17
107.53(d)(7)(i) Control Measures to Prevent Delivery of Unauthorised Article to Screened Persons. ....	17
107.53(d)(7)(ii) Control Measures to Prevent Delivery of any Firearm to Screened Persons. ....	17
107.53(d)(7)(iii) Control Measures to Prevent Delivery of any other Dangerous or Offensive Weapons to Screened Persons.....	17
107.53(d)(7)(iv) Control Measures to Prevent Delivery of any Ammunition to Screened Persons. ....	17
107.53(d)(7)(v) Control Measures to Prevent Delivery of Unauthorised Articles to Screened Persons.....	17
107.53(d)(8) Designed of Sterile Areas .....	18
107.53(d)(9) Security awareness Training for staff including contacted personnel .....	18
107.53(d)(10) Identifying and Reporting Security Breaches and Deficiency to the Director.....	18
107.53(d)(11) Provisions for the Security of Services.....	18
107.53(d)(12)(1)(i) – (iii)_ Measures to Prevent, Respond and Rectify Cyber- Attacks .....	19
107.53(d)(13) Perimeter Signs.....	20
107.53(d)(14) Screening of Persons Other than Passengers .....	21
107.53(d)(15) Vehicle Access to Security Restricted Areas or Security Enhanced Areas .....	21
107.53(d)(16) Randomness and Unpredictability Measures.....	24
107.53(d)(17) Identification System.....	25
107.53(d)(18) Screening for Persons Other than Passengers.....	25
107.53(d)(19) Method of detecting explosives and explosive devices .....	26
107.53(d)(20) Merchandise and supplies introduced into SRA.....	27
107.53(d)(20) Procedures for unidentified baggage and suspicious in a accordance with a risk assessment .....	27
07.53( e)(1) Security Designated Airport Barrier Protection.....	28
107.53( e)(2) Control and Monitoring of Landside Threats .....	28
107.53( e)(3) Prevent Inadvertent Unauthorised Access .....	29
107.53( e)(4) Security Services Airport Identity Card Procedure.....	31
107.53( e)(5) Cyber Security Procedures for Airport Development.....	31
107.53( e)(6) Access Control Procedures .....	31
107.53( e)(7) Screening Procedures.....	31
107.53( e)(8) Training Programme .....	31
107.53( e)(9) Procedures for Incident Notification.....	32
107.53( e)(10) procedures for Liaison with Other Organisations .....	32
107.53( e)(11) Airport Identity Card Procedure .....	32
107.53( e)(12) Procedures for Airport Development.....	32
107.53( e)(13) Procedures Airport Emergency Plan – Security Related Events.....	32
107.53( e)(14) Procedures to Minimize Unlawful Interference .....	32

107.53( e)(15) Procedure for Increased Level of Security Risk .....	32
107.55 Access Control.....	33
107.55(1) Insecure Door, Gates and Barriers of Access Control.....	33
107.55(2) Measures for Articles Capable of Facilitating the Evasion of Control Measures. ....	33
107.57 Screening .....	33
107.57(a)(1) Authority to Conduct Screening .....	33
107.57(a)(2) Screening of Passenger, Crew Member and Baggage for Aircrafts Operation from or within Papua New Guinea. ....	34
107.57(b) Screening of Non-Passengers, Vehicle and Goods .....	34
107.59 Training of Personnel .....	34
107.59(a)(1) Training Programme .....	34
107.59(a)(2) Initial and Recurrent Training.....	35
107.59(a)(3) Maintenance of Training Records.....	35
107.59(a)(4) Standard of Performance for Initial and Periodic Assessments .....	35
107.59(a)(5) Assessment for Competencies for Initial and Recurrent Training .....	36
107.59(b)(1) Applicable Segments for Initial and Recurrent Training .....	36
107.59(b)(2) Knowledge Testing or Competency Assessment.....	36
107.59(c )(1) Training Syllabus.....	36
107.59(c )(2) Authorisation to conduct training .....	36
107.59(c )(3) Instructor qualification and Certification.....	36
107.59(d ) Recurrent Training Interval.....	36
107.59(e)(1) Records of Persons Authorized to Conduct Training .....	36
107.59(e)(2) Records of Persons Undertaking Security Training.....	36
107.59(f)(1) Record of Name of Persons Attending Training .....	37
107.59(f)(2) Record of Instructor Competencies, Experience and Qualifications. ....	37
107.59(f)(3) Record of Scope of Training .....	37
107.59(g)(1) Record of Name and Date of Birth of Person Conducting Training.....	37
107.59(g)(2) Record of the Identity of the Training Segment .....	37
107.59(g)(3) Record of Attendance, Instructor Comments, Test Results and Assessments .....	37
107.59(h)(1) Accurate, Legible and Permanent Nature Records .....	37
107.59(h)(2) Record Retention Period.....	37
107.61 Incident Notification and Reporting .....	37
107.61(1) Incident notification are complied with requirements of rule Part 12 .....	37
107.61(2) Incident Notification Liaison with Other Organization.....	37
107.63 Liaison with Other Organizations .....	38
107.63(a)(1) Liaison and Consultation with Other Organization involved in Contingency Planning. ....	38
107.63(a)(2) Establishing Airport Security Committee .....	38
107.65 Airport Identity Cards.....	38
107.65 (a) Directors Approval for Issue of Airport Identity .....	38

---

107.65(b)(1) Background checks.....	38
107.65(b)(2) Recurrent Background Checks .....	41
107.65(b)(3) Persons Found Unsuitable by Background Checks. ....	41
107.65 (d) Authorised Persons for Security Restricted and Security Enhanced Areas .....	42
107.65(d)(1) Wearing of Airport Identification Card .....	42
107.65(d)(2) Another Identity Document .....	43
107.65(e) Holders Name Not Disclosed .....	43
107.65(f) Authorised Persons in Security Area .....	43
107.65(g) Airport Identity Card Inspection .....	43
107.65(h) Holder of an Airport Identity Card Cease of Employment .....	43
107.65(i)(1) Crew of Aircraft Engaged in International Operation .....	44
107.65(i)(2) Official of a Papua New Guinea Government Agency on Official Duties .....	44
107.65(i)(3) Passengers Entering Security Restricted Areas .....	44
107.65(i)(4) Pilot In Command of Aircraft not Engaged in Air Operations .....	44
107.65(j) Updating Security Features and Design of Approved Airport Identification Card .....	44
107.67 Airport Development .....	45
107.69 Vehicle Passes .....	46
107.69(1) Vehicle Permit System .....	46
107.69(2) Period Renewal of Vehicles Passes.....	47
<b>Subpart C — Transition Provisions .....</b>	<b>49</b>
<b>APPENDIX A – Model Airport Security Programme.....</b>	<b>49</b>

## Subpart A — General

### 107.1 Purpose

Part 107 applies to any entity or organization that operates an Airport that has been designated as a Security Designated Airport by the Minister, in accordance with Section 153 of the Civil Aviation Act 2000 (as amended).

### 107.3 Definitions

The definitions section contains only those definitions that have a specified meaning relevant to Part 107. Other generally used definitions can be found in:

- (1) Part 1, Definitions and Abbreviations,
- (2) Civil Aviation Act 2000 (as amended)
- (3) National Civil Aviation Security Programmes (Version 8.0, April 2025 ) other PNG legislation, if appropriate
- (4) Security Designated Airport means an Airport designated by the Minister as a Security Airport under Section 153(1) of the Civil Aviation Act 2000 (as amended).

Annex 17 to the Convention on International Civil Aviation and ICAO Document 8973 Security Manual has been used as the basis for defining relevant aspects of the Rule.

## Subpart B — Airport Security Programme Requirements

### 107.51 Airport Security Programme

This is the general introductory requirement leading into the specific Airport Security Programme (ASP) requirements.

#### 107.51(a)(1): Airport Plan

The holder of an Airport Operating Certificate must contain maps and diagrams that clearly show and / or identify security related areas of the Airport, whether established under law or otherwise. These would include; airside, landside, access control points, established security restricted areas, terminal floor plans, screening point locations and sterile areas and the plan of the Airport and its facilities as required by rule 139.5(3)

#### 107.51(a)(2) Airport Grid Map

The holder of an Airport Operating Certificate is required to have a grid map of the Airport and its immediate vicinity required by rule 139.57(b)

#### 107.51(a)(3) Map of the Airport

The holder of an Airport Operating Certificate must have a map of the Airport clearly showing:

- (i) The airside and landside boundary

#### Access to Airside from Non- Terminal Locations

The Airport Operator is required to develop procedures to ensure that access control measures with regard to each access point to the airside are effectively implemented.

The ASP must provide sufficient details in regard to the measures to be taken for access control to the airside from the non- terminal location and may be considered as vulnerable points, such as:

- (a) Cargo areas
- (b) Maintenance facilities
- (c) General aviation facilities
- (d) Catering facilities
- (e) Fuel farms
- (f) All designated staff and vehicle access control checkpoints, etc.
- (g) Pedestrian and vehicle gates

A vulnerable point is any facility on or connected to an airport that, if damaged or destroyed, would seriously impair operations. Air traffic control towers, communication facilities, radio navigation aids, power transformers, primary and secondary power supplies and fuel installations, both on and off the airport, should be considered vulnerable points. Communication and radio navigation aids that could be tampered with should be accorded a higher level of security.

If such installations cannot be adequately protected by physical security measures and intrusion detection systems, they should be visited frequently by security staff or maintenance technicians. Staffed installations should have strict access control measures, and admission to such installations should include the requirement to produce a valid identification permit.

A lock and key control system and electronic access system with card readers should be established at each airport. Such a system should identify the type of lock and key and access used, such as master, grand master, numbered or registered to prevent duplication. Additionally, special procedures should be defined for the issuance, usage and protection of keys, and be followed in the event of loss. If airport tenants have their own key systems, their systems should be synchronized and used with the agreement of the airport authority. Special procedures to be followed in case of an emergency should also be established.

- (ii) a detailed map of any declared security areas or enhanced security areas; and
- (iii) access control points in the boundary, including hangars and other facilities that have direct access to the airside which may be leased to third parties; and
- (iv) The diagram showing location of any isolation parking
- (v) Declared security restricted areas or security enhanced areas are declared in accordance with a risk assessment carried out the by the relevant authority.

#### **107.51(a)(4) Terminal Diagram Access Points**

The holder of an Airport Operating Certificate must have a diagram of the terminal(s) clearly showing access control points and sterile areas.

- Access Control Points to airside or a security restricted area include;
  - All doors, stairs and passenger loading bridges
  - Staff Access Doors;
  - Departure Access Points;
  - Emergency Doors
  - Baggage Conveyor Belts

- Effective communication systems;
- Access Points at cargo areas, maintenance facilities, general aviation facilities, catering facilities, including pedestrian and vehicle gates, etc.

**107.51(b)(1) Required Personnel**

The ASP is required to have the details, duties and responsibilities of personnel required by rule 139.51

**107.51(b) (2) Positions Responsible for Training of Personnel**

The holder of an Airport Operating Certificate is required to list the position(s), identified in rule 107.59(c)(2), that is/are responsible for training personnel, in accordance with the security training programme required by rule 107.59.

**107.51(b)(3): Identifying Key Airport Stakeholders**

The holder of an Airport Operating Certificate is required to identify the key stakeholders with a clear delineation of who is responsible for the achievement of aviation security outcomes.

**107.51(c): Current Contacts of Airport Stakeholders**

The holder of an Airport Operating Certificate must contain contact details for all stakeholders and regularly monitor these contact details to ensure that they remains current to allow a timely response to any security incident or event.

**107.51 d: Management of Security Sensitive Information**

The holder of an Airport Operating Certificate must contain details of how information is shared among stakeholders, while recognizing that the distribution of security sensitive information needs to be managed in accordance with appropriate procedures to ensure it is restricted to those with a genuine ‘need to know’ that information. Once shared, such information is to be appropriately stored or destroyed.

**107.51(5): Airport Security Committee (ASC)**

The holder of an Airport Operating Certificate is required to outline the details of the establishment of an Airport Security Committee.

An Airport Security Committee is required to establish procedures to review the continued effectiveness of airport security measures, based on a security risk assessment analysis, recent events and the results of quality control activities. The ASC should also serve as a forum to coordinate airport security arrangements, and discuss operational issues and concerns regarding the implementation of routine security measures, as well as those for major ad hoc events. An ASC may also advise the airport security authority on issues related to airport security.

**107.51(e )(1) Terms of Reference of ASC**

The Terms of Reference of an ASC must include the responsibility to:

- (a) coordinate the implementation of the NCASP at the airport;
- (b) oversee and monitor the ASP, including special measures introduced by the airport authority, operators and airport tenants;



- (c) identify vulnerable areas, including essential equipment and facilities, and review the security of these areas on a regular basis;
- (d) ensure that security measures and procedures in place are adequate to meet security risks and that they remain under constant review, providing for normal situations and contingencies for periods of heightened security and emergency situations;
- (e) arrange for security inspections and tests to be carried out on an unpredictable but frequent basis;
- (f) ensure that recommendations for improvement in security measures and procedures are implemented;
- (g) inform the Director of Civil Aviation of Papua New Guinea of the current state of security measures and procedures in effect at the airport, and refer to the Director any problems related to the protection of the airport and its services which cannot be resolved at the airport level
- (h) arrange for the security education and training of airport staff; and
- (i) ensure that any plans for airport expansion include plans for modifications to be made to airport control systems and equipment.
- (j) Lists the composition of members (stakeholders) of ASC

#### **107.51(e )(2) Composition of Members of ASC**

The holder of an Airport Operating Certificate is required to list and detail the composition of the ASC members including stakeholders and agencies.

#### **107.51(e )(3) Frequency of ASC Meeting**

The holder of an Airport Operating Certificate is required to ensure that the frequency of ASC meetings must be adapted to the needs of the airport. An ASC should meet at least four times per year and, whenever necessary, convene meetings with smaller focus groups.

#### **107.51(e )(4) Management of Meeting Records**

The holder of an Airport Operating Certificate is required to detail the procedure for recording, maintaining and distribution of Airport Security Committee meeting minutes.

#### **107.51(f): Details of Measures and Procedures**

The holder of an Airport Operating Certificate must describe in detail the measures and procedures required by the following Rule Part;

- (1) 107.53 regarding security requirements;
- (2) 107.55 regarding access control;
- (3) 107.57 regarding screening;
- (4) 107.59 regarding the security training programme;
- (5) 107.61 regarding incident notification and reporting;
- (6) 107.63 regarding liaison with other organization;
- (7) 107.65 regarding airport identity cards;
- (8) 107.67 regarding Airport development.

#### **107.51(g) Contractual Provisions**

The holder of an Airport Operating Certificate must contain the contractual arrangements by which the Airport Operator will ensure that any contractor or agent involved in the handling of the

Airport Services will comply with the security programme of the Airport. The specific content of any standard clause in a contract with the contractor or agent will normally be sufficient. Such contractual arrangements with respect to airport tenants need to be documented to clarify responsibility and accountability.

#### **107.51(h) Periodic Verification of Security Measures Outsourced to External Service Providers**

The holder of an Airport Operating Certificate must establish procedures to ensure that each holder of an Airport Certificate responsible for implementation of relevant elements of the National Civil Aviation Security Programme must periodically verify, at intervals of not more than 12 months, the implementation of security measures outsourced to external service providers in compliance with the certificate holder's airport security programme.

#### **107.51 (i) periodic review of the Airport Security Programmes**

The holder of an Airport Operating Certificate is required to develop and implement procedures to ensure periodic review of the airport security programme is conducted, including their amendment as required.

#### **107.51(j) Distribution of the Airport Security Programmes**

The holder of an Airport Operating Certificate is required to develop and implement procedures for the distribution to all aircraft operators providing service from all airports in Papua New Guinea and other relevant airport-level stakeholders, are provided with and have copies of the relevant portions of the airport security programme.

### **107.53 Security requirements**

#### **107.53(a) Airport Security Programme**

The holder of an Airport Operating Certificate of a Security Designated Airport, must include security measures and procedures to safeguard the public, passengers, crew, ground personnel, aircraft and facilities against an act of unlawful interference.

### **Barrier Requirements**

#### **107.53(b): Safeguards for Preventing Inadvertent Unauthorized Access**

The holder of an Airport Operating Certificate for a Security Designated Airport, in addition to Rule 139.71, must establish procedures to provide safeguards for preventing inadvertent unauthorized access and for deterring intentional unauthorized access to any security restricted or security enhanced area within the airport. The ASP for a Security Designated Airport, is to include security measures and procedures to maintain control of access into Security Areas of the Airport.

#### **107.53(c)(1): Physical barrier access points**

The holder of an Airport Operating Certificate is required to detail the physical barriers that are used to control access to the Airport. These consist of fences, gates, doors and other barriers between public and security restricted areas or security enhanced areas with adequate locking or control systems. The Airport Operator at each Security Designated Airport must establish procedures to control access to the security-restricted areas and security enhanced areas of a Security Designated Airport.

**107.53 (c )(2) Control of any Duct, Drains or Tunnel**

The holder of an Airport Operating Certificate for a Security Designation Airport is required to establish procedures to ensure control of the ducts, drains or tunnel giving access to any security areas or a security enhanced area.

**Physical Security Measures**

Both airside and security restricted area perimeters must be delineated and protected by physical barriers. However, if a section of the perimeter of a security restricted area lies adjacent to open areas, including airside areas, that section must be patrolled or kept under sufficient surveillance, in order to detect any unauthorized access and allow for the apprehension of any intruders before they can reach aircraft or essential facilities.

All airside areas, whether or not they form part of a security restricted area, be separated from adjoining terrain by fences or other effective physical security measures.

Each building located on or immediately abutting the security restricted area perimeter must be adequately secured to prevent unauthorized access to the security restricted area. This requires that any openings, such as windows or ventilation ducts that may permit access to the security restricted area, be securely locked or fitted with bars, grilles or screens. Building roofs may also provide a possible route for unauthorized access and must be similarly protected, in particular if roof lines and buildings adjoin security restricted area perimeter fencing.

If natural features such as a body of water or ravine form part of the airside or security restricted area perimeter, they must afford no less protection than that achieved through fencing. Special care is necessary when natural barriers are used to maintain the integrity of the perimeter. For instance, if the adjacent body of water is navigable, foot or vehicular patrols of its shoreline may not be sufficient and should be augmented by patrols using watercraft.

If underground service ducts, sewers and tunnels cross the airside or security restricted area perimeter, entrances to all ducts and manhole covers through which access to airside areas is possible should be secured and periodically inspected or protected by intrusion detection devices.

Physical security measures shall be supported by properly trained personnel, sound and comprehensive contingency planning, and concise, well written security plans and orders.

**107.53(d) Construction and Height of Barrier**

The specification of construction and height of each barrier required by paragraph (b)(1) considering the surrounding topography must, provide an effective measure against penetration of the security area or security enhanced areas and must in no case be less than 2440 millimeters in height and must include anti-climb facilities.

**Perimeter Protection**

When establishing perimeter protection, consideration must be given by the Airport Operator to the method of construction, material used and any additional security features that may be used to increase the effectiveness of the barrier.

Other barrier requirements to consider for effective measures against unauthorised access include;

- (1) **Clear zones** along the perimeter fence/barrier, with a distance of about 3m on both sides of the perimeter fence. They should be kept clear at all times and be free of obstruction that may assist as cover or aid an intruder to climb over the fence.
- (2) A **patrol road** alongside the perimeter fence/barrier to permit both landside and airside mobile patrols. The roads should be well drained and kept free of obstacles at all times.
- (3) **Emergency gates** to allow the quick access of emergency service vehicles to on-airport or off-airport aircraft accidents. Such gates should be constructed to also maintain the integrity and standard of the perimeter fence and therefore should be locked, guarded and under continuous surveillance. Airport Authority may also consider equipping such gates with intrusion detection systems as an additional security measure.
- (4) **Safety and Operational Considerations** at certain locations on the perimeter mean that metal fences cannot be used (particularly adjacent to the take-off and landing runway thresholds), since they might disrupt the operation of navigation aids. Therefore, in this case, special fencing materials or construction methods may be required, such as the use of non-metallic and frangible fencing material, or living fences, i.e. thorny plants, providing equivalent security.
- (5) **Maintenance of fence/barrier**, the ongoing maintenance of the perimeter fence and ease of replacement must be considered during the construction phase, therefore allowing for the most appropriate material to be used.

### **Designation and Establishment of Security Restricted Areas (SRAs)**

The Airport Operating Certificate holder for a Security Designated Airport is required to ensure that its Security Restricted Areas (SRAs) are designated and established in accordance with a security risk assessment carried out by the relevant authorities.

**Designation process**, shall involve the identification of those areas of the airside of an airport which on a security risk assessment are identified as priority risk areas where in addition to access control, other security controls are applied.

**Establishment process** shall involve the setting up of the identified SRA in a manner that it can be effectively secured and monitored at all times, to prevent unauthorized access or entry.

Requires the holder of Airport Operating Certificate, when establishing Security Restricted Areas (SRAs) to ensure;

- (1) security control points into Security Restricted Areas and Airside Areas are also clearly identified and established;
  - Security Control Points into SRA from the terminal building may include; doors, baggage belt openings, passenger boarding bridges, roof accesses and fire exits, staff access points, spectator terraces and/or other areas overlooking SRAs.
  - Security Control Points from non-terminal locations to the airside may include; cargo areas, maintenance facilities, general aviation facilities, catering facilities, pedestrian and vehicle gates, etc.

- 
- (2) the appropriate security access control measures and procedures into SRA and Airside Areas must be established and implemented at all times. The following security control measures shall be considered based on applicability and the security risk assessment conducted:
  - *Clear demarcation of the security restricted area boundary*; allowing for the implementation of higher access control standards to be applied to monitoring persons and vehicle access and movement within the SRA.
  - *Access control points into the SRA* must be equipped with the necessary access control measures to deter unauthorized access and prevent the introduction of unauthorized items. Access Control Points include:
    - All doors, stairs and passenger loading bridges
    - Staff Access Doors;
    - Departure Access Points;
    - Emergency Doors
    - Baggage Conveyor Belts
    - Effective communication systems;
    - Access Points at cargo areas, maintenance facilities, general aviation facilities, catering facilities, including pedestrian and vehicle gates, etc.
  - Vulnerability points; should be accorded a high level of security protection and control measures.
  - Lock and key controls; if established, must have clearly defined procedures for issuance, usage and protection.
  - Physical Security Control Measures; ensure that necessary physical barriers and measures are established to prevent unauthorized access into SRAs:
    - any openings, such as windows or ventilation ducts that may permit access to the security restricted area, be securely locked or fitted with bars, grilles or screens.
    - If underground service ducts, sewers and tunnels cross the airside or security restricted area perimeter, entrances to all ducts and manhole covers through which access to airside areas is possible should be secured and periodically inspected or protected by intrusion detection devices.
    - Physical security measures should be supported by properly trained personnel, sound and comprehensive contingency planning, and concise, well written security plans and orders.
  - The use of relevant security control systems:
    - Airport Security Identification Permit (ASIP)/ Airport Security Identification Card (ASIC) System; to ensure that only authorised personnel are to access the SRAs. This card or documentation is issued by Airport operator to individuals employed at the airport or persons

who have a need for authorised access to the Airport, airside or security restricted area. All persons must meet the ASIP/ASIC requirements prior to being issued the permit/card.

- Vehicle Permit System; to ensure that only authorised vehicles are to access the SRA.
  - Automated access control system; ensures that authorised and valid personnel are to access the SRA
  - CCTV Surveillance Coverage; provides addition oversight on SRA areas and may be interconnected to the Security Identification Permit System.
  - Intrusion Detection System; assists in the detection or attempted entry of an intruder into the SRA. It identifies the location of the intrusion and signals or generates an alarm to a response force. It can be and is more effective when integrated with the CCTV system.
- *Lighting*; there must be sufficient illumination or lighting established and provided in the terminal area, perimeter barrier, ramp areas, cargo areas, maintenance facilities and pedestrian and vehicle gate areas during hours of darkness.
  - *Security Emergency Response Plan*; security response plans and procedures shall also be available at the different security checkpoints as personnel deployed to monitor the access points and conduct/implement the security measures must ensure that in the event of security incidents and emergencies the correct response procedures are implemented accordingly.
  - *Security Personnel*; deployed at the security control points must be adequately trained to implement the security control measures as well as be able to respond effectively and efficiently to any security breaches at the security control points.

- (3) A security risk assessment should be conducted to establish the security control points and the appropriate security access control measures to be applied at each security control point.

### **107.53(d)(1) Isolated Parking Position**

The holder of an Airport Operating Certificate must document and establish in the ASP and designate an isolated aircraft parking position at their Airport for the parking of an aircraft that is known or believed to be subject of unlawful interference, or which for other security reason needs isolation from normal Airport activities (see CAR Part 139 Appendix C9);

An aircraft suspected of having an explosive device or dangerous substance on board shall be isolated from normal aircraft operations. Each airport must therefore designate one or more isolated aircraft parking positions to which such an aircraft may be moved. The site selected shall be the maximum distance possible, or a minimum of 100 meters, from any other aircraft parking position, runway, taxiway, building, public area, fuel tank farm or storage area for explosive or incendiary material.

An isolated aircraft parking position shall also be used to manage an aircraft subjected to an act of unlawful interference that requires servicing or special attention. Therefore, consideration must be given to selecting a location that cannot be easily observed from public areas.

Signage that may reveal the location of the isolated parking position must not be visible to the public.

Care must be taken to ensure that there are no services such as gas pipelines, refueling hydrant pipes, other fuel lines or electric power cables beneath the aircraft parking position surface. If possible, a second isolated parking position should be designated in case the primary isolated parking position is unavailable or there are multiple incidents.

Consideration must also be given to the prevailing wind direction and aircraft landing and take-off routing at the airport, so as to minimize disruption to airport operations and the surrounding locality in the event of a security incident or an aircraft fire or release of dangerous substances from an aircraft.

Airport emergency procedures must also designate one or more points to which an aircraft subjected to an act of unlawful interference might be directed. However, plans should be flexible enough to allow for the aircraft to change its position if necessary. The following must be taken into account in selecting designated points:

- (a) availability of covered approaches to facilitate action by security forces, for example, adjacent buildings and natural features such as trees and undulations in the terrain;
- (b) need for police and other units to have quick and easy access to the area to deal with the incident;
- (c) possible danger to people or other aircraft in the vicinity, and hazards such as fuel tanks;
- (d) need for isolation from the press and public; and
- (e) continuance, as far as possible, of normal air traffic in and out of the airport during the incident and re-establishing business as usual after the incident.

### **107.53(d)(2) Emergency Lighting**

The holder of an Airport Operating Certificate is required to provide and maintain adequate lighting, and emergency lighting in the event of failure of the normal lighting system.

Sufficient lighting must be provided for any parking areas at their Airport used at night by aeroplanes having a certificated seating configuration of 20 seats or more passengers, excluding any required flight crew member seat, that are engaged in scheduled air transport operations for the carriage of passengers. Aircraft parked overnight shall be parked in controlled and well-illuminated areas. Illumination fixtures, in addition to being connected to the airport's main power supply, should be connected to a secondary power supply. Alternatively, portable lighting must be readily available for use when the main power supply is disrupted.

Aircraft parked overnight must be observed by irregularly timed patrols carried out by Airport or Aircraft Operator security staff or law enforcement officers. Patrols are particularly effective during low-level airport operations when only a small number of authorised people are working.

**107.53(d)(3) Potable Lighting for Designated Aircraft Parking Areas**

The holder of an Airport Operating Certificate is required to establish procedures to provide lighting, or have portable lighting available within 30 minutes, on any designated isolated aircraft parking area at their Airport intended to be used at night.

**107.53(d)(4)(i) Screening of International Passenger, Crew and their Baggage**

The holder of an Airport Operating Certificate for each Airport Operator is required to provide an area for the screening of international passengers, crew and their baggage prior to aircraft boarding.

All passengers and cabin baggage, including transfer passengers and baggage, must undergo appropriate security screening before being allowed access to an aircraft, sterile area or security restricted area.

**107.53(d)(4)(ii) Sterile areas for International Passengers**

The holder of an Airport Operating Certificate for each Airport Operator must provide/designate an area as a sterile area where international passengers and crew subjected to screening are prevented from having access to unauthorised articles or contact with unscreened persons:

Where the screening of passengers and their carry-on baggage is required by the Director, the Airport operator must establish a sterile area for holding passengers after they have been screened and cleared of any threats and until they board the aircraft. This area must be designed in a way as to ensure that access is strictly controlled and there is no mingling of screened and unscreened passengers, including arriving passengers.

**107.53(d)(4)(iii) Mixing of screened and unscreened persons**

The holder of an Airport Operating Certificate for each Airport operator is required to provide/designate an area for the separation of arriving passengers and crew from departing passengers during international deplaning to prevent arriving, transit, and transfer passengers and crew having contact with any person who has been subject to screening.

Security measures shall be implemented for international flights to ensure that there is no mixing or contact between passengers subjected to security controls and other persons not subjected to such controls, after a security screening checkpoint has been passed.

In the event of a mix of screened and unscreened passengers, the following action shall be taken:

- (a) the sterile area shall be cleared and a full search carried out by the airport operator or its delegate;
- (b) departing passengers and their cabin baggage shall be required to undergo a second screening process before being allowed to board their aircraft;
- (c) should any departing passenger have had access to an aircraft after the occurrence of the accidental mix, the aircraft concerned shall also be subjected to a full cabin search.



**107.53(d)(5) Enhanced Security Areas**

The ASP must include, when considered necessary by the Director, areas at their Airport for the screening and searching of persons, items, substances, and vehicles entering and remaining within security areas or enhanced security areas.

**107.53(d)(6) Security threat**

The holder of an Airport Operating Certificate is required to ensure that when considered necessary by the Director to respond to a security threat, provide areas at their Airport for the screening of international passengers, crew and their baggage and for the screening of domestic passengers, crew and their baggage

**107.53(d)(7)(i) Control Measures to Prevent Delivery of Unauthorised Article to Screened Persons.**

The holder of an Airport Operating Certificate is required to ensure that concession areas at their Airport that are situated in an area accessible to screened passengers are designed in such a way that they provide access control measures sufficient to prevent delivery to any screened person of any unauthorized article.

**107.53(d)(7)(ii) Control Measures to Prevent Delivery of any Firearm to Screened Persons.**

The holder of an Airport Operating Certificate is required to ensure that concession areas at their Airport that are situated in an area accessible to screened passengers are designed in such a way that they provide access control measures sufficient to prevent delivery to any screened person of any firearm.

**107.53(d)(7)(iii) Control Measures to Prevent Delivery of any other Dangerous or Offensive Weapons to Screened Persons.**

The holder of an Airport Operating Certificate is required to ensure that concession areas at their Airport that are situated in an area accessible to screened passengers are designed in such a way that they provide access control measures sufficient to prevent delivery to any screened person of any other dangerous or offensive weapons or instrument of any kind.

**107.53(d)(7)(iv) Control Measures to Prevent Delivery of any Ammunition to Screened Persons.**

The holder of an Airport Operating Certificate is required to ensure that concession areas at their Airport that are situated in an area accessible to screened passengers are designed in such a way that they provide access control measures sufficient to prevent delivery to any screened person of any ammunition.

**107.53(d)(7)(v) Control Measures to Prevent Delivery of Unauthorised Articles to Screened Persons.**

The holder of an Airport Operating Certificate is required to ensure that concession areas at their Airport that are situated in an area accessible to screened passengers are designed in such a way that they provide access control measures sufficient to prevent delivery to any screened person of any explosive substance or device, or any injurious substance or device of any kind that could be used to endanger the safety of an aircraft or of the persons on an aircraft;

Where concession areas / retail outlets are provided for within a sterile area, consideration must be given to their location and design to ensure that no prohibited items, such as knives and scissors that may be required for food preparation (as an example), are accessible by screened passengers.

#### **107.53(d)(8) Designed of Sterile Areas**

The holder of an Airport Operating Certificate is required to design all areas such a way that they provide access control measures sufficient to prevent any unauthorised persons from entering the area.

#### **107.53(d)(9) Security awareness Training for staff including contacted personnel**

The holder of an Airport Operating Certificate must establish policies and procedures to ensure that personnel engaged, employed or contracted by the certificate holder undergo a security awareness programme, and that each person required to carry out specific security tasks is trained for those tasks in accordance with the security training programme require by rule 107.59.

The holder of an Airport Operating Certificate must consider developing and implementing a security awareness training programmes for all employees working within the operational environment to raise awareness of the prevailing security situation within each airport environment. Activities shall include regular security awareness training, refresher courses and security briefings.

In collaboration with CASAPNG, Airport Operators should implement robust security culture programmes for all airport employees. In order to establish or improve security culture in organizations, measures should be developed to enhance such norms, beliefs, values, attitudes and assumptions, provide mechanisms for reporting suspicious activities and behavior, and encourage staff to use such mechanisms

#### **107.53(d)(10) Identifying and Reporting Security Breaches and Deficiency to the Director.**

The holder of an Airport Operating Certificate is required to establish procedures for identifying, reporting to the Director, and dealing with, breaches of and deficiencies in, any security procedures established by the Airport certificate holder and any provisions of any enactment relating to security at the Airport.

The security reporting system is to collect information as reported by personnel to improve the level of security performance. It may assist in identifying deficiencies, incidents or unsatisfactory performance, and aim to encourage individuals to report incidents and deficiencies that would otherwise remain unnoticed and would therefore not be corrected.

#### **107.53(d)(11) Provisions for the Security of Services**

The holder of an Airport Operating Certificate is required to establish procedures to make provision for the security of services including, but not limited to, energy supplies, communications, sewerage and water supplies, in order to minimize the risk of such services being used to interfere unlawfully with aviation operations.

#### **Vulnerable points**

A vulnerable point is any facility on or connected to an airport that, if damaged or destroyed, would seriously impair operations. Air traffic control towers, communication facilities, radio navigation aids, power transformers, primary and secondary power supplies and fuel installations,

both on and off the airport, should be considered vulnerable points. Communication and radio navigation aids that could be tampered with should be afforded a higher level of security.

If such installations cannot be adequately protected by physical security measures and intrusion detection systems, they should be visited frequently by security staff or maintenance technicians. Staffed installations should have strict access control measures, and admission to such installations should include the requirement to produce a valid identification permit

Airport Operators are expected to undertake a security risk assessment to determine the boundary of any landside area that they intend to exercise control over. It should be noted that this may not comprise the entire land envelope owned by the airport but should consider terminal roadways, carparks and any operational infrastructure that is not in a designated secure area.

### **107.53(d)(12(1)(i) – (iii)\_ Measures to Prevent, Respond and Rectify Cyber- Attacks**

The Airport Operator is required to establish procedures to ensure appropriate steps are taken to minimize the threat to civil aviation operations, including measures to prevent, respond to and rectify cyber-attacks and corruption of information technology systems.

Airport Operators are expected to undertake a security risk assessment to determine critical infrastructure that could be the target of any cyber-based attack. Risk mitigation strategies should be developed that allow for the detection and interruption of any attack, contingencies for dealing with the outcomes of any attack and measures to re-establish operations as soon as possible after an attack.

## **1. Identification & Classification**

- Inventory of Critical Assets
  - Identify and maintain an up-to-date inventory of ICT systems and data critical to aviation safety, security, and operations.
- Classification by Criticality
  - Classify assets based on operational impact (e.g., safety-critical, security-critical, facilitation-critical).

## **2. Risk Assessment**

- Holistic Threat Modeling
  - Conduct structured, risk-based threat assessments to identify potential threats and vulnerabilities in accordance to AVSRAM Document.
- Risk Register
  - Maintain a centralized register of risks and associated mitigation measures.

## **3. Protective Measures**

### **(a) Administrative Controls**

- Policies, Procedures, and security awareness training
- Defined roles, responsibilities, and segregation of duties
- Personnel vetting and background checks

### **(b) Technical Controls**

- Firewalls, IDS/IPS, and endpoint protection

- Network segmentation for safety and security domains
- Data encryption (in transit and at rest)
- Multi-factor authentication and strict access controls

(c) Physical Controls

- Secure data centers and server rooms with limited access
- Surveillance and intrusion detection systems
- Access logs and physical entry controls

#### **4. Continuous Monitoring**

- Implement Information Security Continuous Monitoring (ISCM)
- Use Security Information and Event Management (SIEM) systems
- Perform routine log analysis, vulnerability scans, and system audits

#### **5. Incident Detection & Response**

- Real-time monitoring and alerting of anomalies
- Clear incident response plan with severity classification
- Crisis communication plan and notification protocols
- Post-incident review and lessons learned

#### **6. Supply Chain Security**

- Vet suppliers for cybersecurity practices
- Include security clauses in contracts and SLAs
- Monitor third-party compliance and system updates

#### **7. Training & Awareness**

- Regular cybersecurity training for all aviation stakeholders
- Specialized training for ICT personnel and incident responders
- Simulation exercises (e.g., Tabletop Exercises)

#### **8. Post Event Analysis**

- Once an incident response has been concluded and aviation operations restored to a normal operating mode, conducting a thorough analysis of the event is a critical step in ensuring that there is no future recurrence.
- Analysis should be performed with third party system providers, manufacturers or appropriate authority to help identify the root causes and identify cross-references to existing safety analyses/documentation.
- All findings and final recommendations should be shared with states and the aviation industry stakeholders so that they may adjust their respective cybersecurity governance approach and programme.

#### **107.53(d)(13) Perimeter Signs**

The holder of an Airport Operating Certificate is required to display signage when so required by the Director, and to affix signs at the perimeter of security restricted areas or enhanced security areas within their Airport.

The Airport Operator shall ensure that appropriate signage is strategically placed and visible in order to remind all persons to be on alert for suspicious activities, prepared for emergencies or otherwise informed of security measures in place. Signs must also be placed in the landside areas and other public areas for information awareness and warning.

#### **107.53(d)(14) Screening of Persons Other than Passengers**

The holder of an Airport Operating Certificate is required to establish a process to ensure screening of persons other than passengers, together with items carried, prior to entry into a security area or an enhanced security area serving international civil aviation operations are subject to screening and security controls, with the percentage of screening determined by a security risk assessment carried out by the Airport Operator.

The application of proportional screening and other security controls, randomness and unpredictability to persons other than passengers and the items they carry should be determined on the basis of risk.

The proportion of non-passengers to be screened (*which may include 100 per cent screening*) should be determined on the basis of security risk assessments by the Airport Operator and approved by the Director. This proportion may vary from airport to airport within Papua New Guinea.

Screening and other security controls applied to a proportion of non-passengers and the items they carry entering and within security restricted areas should be applied in such a way that they allow for randomness and unpredictability. Randomness and unpredictability should be applied to achieve a greater deterrent effect of security measures. For there to be a real deterrent effect, there should be a significant chance that any person may be subjected to screening and other security controls at any time, and no person should be able to avoid, or aid others to avoid, the security controls being applied.

When applying random and unpredictable screening and/or security controls, “random” is understood to ensure an equal probability for each non-passenger to be subjected to screening or other security controls, while “unpredictable” is understood to describe measures applied at irregular frequencies, different locations and/or with varying means, for the purpose of increasing deterrence and effectiveness. Randomness should not convey any lack of aim or purpose, lack of direction or lack of conscious choice. In all cases, screening and other security controls carried out in a random and unpredictable manner should achieve outcomes to combat the insider threat as presented above and be applied in a deliberate manner supported by a security risk assessment and documented methodology.

#### **107.53(d)(15) Vehicle Access to Security Restricted Areas or Security Enhanced Areas**

The holder of an Airport Operating Certificate for a Security Designated Airport is required to establish procedures for granting access to secure restricted areas, or security enhanced areas for vehicles together with the items contained in term are subjected to screening or other appropriate security controls required by the Director.

**Screening of Vehicles and Supplies Conveyed in Security Restricted Areas.**

Vehicles and items carried within them must be subjected to screening or other appropriate security controls before entering a security restricted area, in accordance with a security risk assessment carried out by the relevant national authorities and the airport Operator.

**Security outcome**

The screening or other appropriate security controls on vehicles must reasonably ensure that a vehicle does not carry any unauthorised person or unauthorised prohibited item when entering security restricted areas.

The implementation of screening or other security controls for vehicles and items carried within is intended to reasonably ensure that unauthorised persons, or prohibited items that could be used to carry out an act of unlawful interference, are not introduced into a security restricted area. The measures to be applied should be based on the results of security risk assessments carried out by the Airport Operator, and approved by the Director.

**Verification of Authorisation**

Only vehicles with an operational reason shall be allowed to enter a Security Restricted Area.

The occupants of a vehicle seeking access to a security restricted area must carry valid authorization (airport security identification permit or equivalent). In addition, vehicles must hold a valid authorisation (vehicle identification or permit) or be escorted by authorised vehicles and personnel.

A verification should be performed by the access point personnel to ensure that the authorisation being presented corresponds to the vehicle and occupants of the vehicle seeking access to the Security Restricted Area.

**Prohibited item list**

Some prohibited items may be necessary for the occupants of a vehicle to bring into a Security Restricted Area, whether frequently or infrequently (e.g. tools of the trade, tools used for construction works in the Security Restricted Area). States should therefore consider establishing the approved list of prohibited items that are authorised inside Security Restricted Areas, based on a security risk assessment carried out by the airport operator and taking into consideration the local environment (e.g. construction workers). Appropriate procedures to be applied to those prohibited items should also be developed (*e.g. visual inspection of tools should be carried out to ensure that they are in fact on the list of prohibited items authorized inside the security restricted area*).

**Screening and other security controls methodology**

The Airport Operator must implement identification checks of all vehicles entering a Security Restricted Area, and verify the validity of all Airport Security Identification Permits of persons seeking access to the Security Restricted Areas.

If less than 100 per cent of vehicles entering the Security-Restricted Area are screened, a proportional selection of vehicles should be made in accordance with a security risk assessment carried out by the Airport Operator and or CASAPNG AVSEC Branch. The principles of randomness and unpredictability should be applied to vehicle screening, in accordance with

defined and documented methodologies, to ensure that all vehicles have an equal probability of being selected for screening.

The driver and any other occupants of a vehicle must not be in the vehicle when screening takes place. They must be required to take their personal belongings out of the vehicle with them, and both occupants and their personal belongings must be subjected to screening procedures.

When a vehicle is selected for screening, it is recommended that a combination of a minimum of three of the following areas of such vehicles be searched in accordance with the principles of randomness and unpredictability, and based on a security risk assessment carried out by the relevant authorities:

- (a) front door pockets, sun visors and glove compartments;
- (b) seat pockets, foot wells and areas underneath seats;
- (c) trunk/boot/baggage/cargo areas; d) wheel arches;
- (d) engine compartment;
- (e) the underside; and
- (f) any other area of the vehicle not listed above.

A methodology should be defined to ensure the randomness and unpredictability of selection of the areas to be searched. If the applied methodology for defining the search area of the vehicle results in the selection of an area that is sealed in accordance with the NCASP and/or ASP, another area should be selected.

The result of a security risk assessment carried out by CASAPNG and the relevant holder of an Airport Certification should determine the number of areas to be searched. There should be clearly defined documented methodologies to ensure that all areas have an equal probability of being searched.

One or a combination of the following methods, as appropriate, should be used to carry out the search of each selected area: a) manual search; b) visual check; and/or c) use of appropriate technologies, such as explosives detection dogs or explosives trace detectors.

A manual search must consist of a thorough manual examination of the area(s) selected, including contents, in order to ensure that they do not contain unauthorised items or IEDs. A visual check could be used as an alternative method of examining empty areas only, such as a glove compartment.

The holder of an Airport Operating Certificate for a Security Designated Airport is responsible for vehicle screening and must also consider providing adequate tools to enable security staff to perform an appropriate examination of the different areas (e.g. mirrors and flashlights).

When areas of a vehicle are sealed in accordance with the National Civil Aviation Security Programme, Airport Security Programme or other approved secure supply chain procedures for the carriage of in-flight supplies, airport supplies or air cargo and mail, such areas may be exempted from screening upon verification of the integrity of the seals and relevant documents, and of the identity of the haulier.

Access to a security restricted area must be denied if the sealed area of a vehicle shows signs of tampering or if inconsistencies in documentation are found (e.g. the seal number does not match the number recorded on the appropriate documentation or the identity of the company or haulier).

carrying in-flight or airport supplies into the security restricted area has not been listed by the airport operator).

Vehicles must be protected from unauthorized access (which includes access from unscreened staff) from the time they have been subjected to screening and/or security controls until entering a security restricted area (including appropriate segregation between vehicles, along with their occupants, subjected to screening and/or other security controls and vehicles, along with their occupants, not subjected to such controls).

A vehicular screening point should ideally have a vehicular control barrier to prevent vehicles from breaking into a security restricted area.

### **Other Security Controls**

Other appropriate security controls may include:

- (a) screening of a proportion of vehicles and items carried within a security restricted area, conducted on a random and unpredictable basis; and
- (b) enhanced patrols and/or surveillance in a security restricted area to confirm that vehicles are holding valid authorization

### **107.53(d)(16) Randomness and Unpredictability Measures**

The holder of an Airport Operating Certificate is required to establish procedures to ensure the use of randomness and unpredictability in the implementation of security measures, as appropriate.

#### **UNPREDICTABILITY PRINCIPLES AND MEASURES**

The application of unpredictability in aviation security can be defined as the implementation of security controls at irregular frequencies, different locations and/or with varying means, in accordance with a defined framework, in order to increase their deterrent effect and their efficiency. These security controls, also called unpredictable measures, should be implemented in such a way that it is highly unlikely for person's subject to such measures (i.e. passengers, non-passengers and, under certain circumstances, the general public) to predict when, where and how they will be applied.

The application of unpredictability in aviation security can help disrupt hostile reconnaissance, surveillance, rehearsal and attack through the deployment of highly visible security controls at locations other than screening checkpoints, and the introduction of unexpected elements to the screening of the general public, passengers and staff, in the overall security framework.

Unpredictable measures within a security regime should be implemented in a manner that is supported by a security risk assessment and documented methodology, with a view to achieving the outcome of thwarting and deterring acts of unlawful interference.

A security risk assessment should therefore be carried out by the airport operator, identifying the types of, and establishing the areas concerned by, unpredictable measures. These measures should be adapted and implemented by airport authority in the airport environment.



**107.53(d)(17) Identification System**

The holder of an Airport Operating certificate for a Security Designated Airport is required to establish and implement an identification system to prevent unauthorised access to the airside and security restricted areas.

- (i) This rule requires the holder of an Airport Operating certificate for a Security Designated Airport must establish an identification system and implement in respect of persons and vehicles in order to prevent unauthorised access to airside and security restricted areas.

Access to the airside and security restricted area of an airport must be controlled by using a security identification permit system. A permit system consists of cards or other documentation issued to individuals employed at airports, or those who otherwise have a need for authorised access to an airport, airside or security restricted area. The system's purpose is to identify the individual and facilitate access, while denying access to unauthorized persons. Vehicle permits are issued and used for similar purposes. Permits are sometimes referred to as airport identification cards or passes.

- (ii) Access must be granted to those with operational need or other legitimate reason to be there. All persons working at an airport will be issued with an identification permit by the Airports Authority. Legislation or regulation should require that airport personnel display their permits at all times while working on the premises. This requirement should apply equally to personnel working in Security Restricted Areas, maintenance areas, catering facilities, air cargo buildings, etc., as well as in the main passenger and airside aircraft handling areas.
- (iii) The identity and authorisation must be verified at designated checkpoints before access is allowed to the SRA and security restricted areas.

As authorised by the Director, the holder of an Airport Operating Certificate is responsible for the design and management of the identification permit system. The use of several different styles of permits should be avoided, as this will pose severe problems for security staff and for the administration of the system. If used in conjunction with an automated access control system, permits may be equipped with electronic or other machine readable codes to allow entry.

Administration of permits

**107.53(d)(18) Screening for Persons Other than Passengers**

The holder of an Airport Operating Certificate is required to establish procedures to ensure that persons other than passengers, together with items carried, must be screened prior to entry into an Airport Security Restricted Areas.

All persons other than passengers, together with items carried, prior to entry to Airport Security Restricted Areas serving international civil aviation operations, shall be subject to screening and other security controls to ensure they are authorised to enter security restricted areas and that they

do not carry prohibited items which could be used to carry out or facilitate an act of unlawful interference.

For the purpose of this guidance material, persons other than passengers include, but are not limited to, airport staff, aircraft operator crew, control authority staff (e.g. Customs and immigration), police officers, visitors, staff of retail outlets, and staff of other ancillary services. Such persons are also referred to as non-passengers or staff in this document, and the terms may be used interchangeably.

Where international operations are occasional rather than continuous, or where there is effective separation of international and domestic operations, screening and other security controls of persons other than passengers and the items they carry may apply only to those persons who are concerned with international operations. In the event that international and domestic operations share a Security-Restricted Area, all non-passengers and items they carry are to be subjected to the international screening and other security control standards.

### Exemptions

For exemption of certain non-passengers from the application of screening and other security controls, in general only in the event that application of screening and other security controls to such persons would negatively impact the safe and secure operation of an airport. Such cases may include emergency services responding to an emergency, and authorized armed officers in the act of escorting a protected person.

### **107.53(d)(19) Method of detecting explosives and explosive devices**

The holder of an Airport Operating Certificate is required to establish procedures to ensure the use of appropriate screening methods capable of detecting the presence of explosives and explosive devices carried by persons other than passengers on their persons or in their items carried. In addition, where these methods are not applied continuously, they shall be used in an unpredictable manner.

Screening of a proportion of non-passengers and the items they carry entering a security restricted area

The Airport Operator may consider implementing a random and unpredictable approach to the screening of a proportion of non-passengers and the items they carry entering a Security-Restricted Area, in order to deter and detect unauthorized prohibited items from being introduced into the security restricted area. The application of additional screening methods, on an unpredictable basis, can enhance the level of security of non-passengers entering the Security-Restricted Area. States may achieve this through a varied application of screening methods and/or techniques (e.g. explosive detection dogs, manual searches, hand-held metal detectors, explosives trace detection and mobile screening units) and/or through the selection of location and frequency where these screening measures may be applied to a proportion of staff selected.

Implementation of random and unpredictable screening of a proportion of non-passengers should be based on a security risk assessment carried out by the relevant authorities and may take into account the individual nature of an airport's operation (*e.g. taking into account shift changes, flight schedules and passenger movements*).

**107.53(d)(20) Merchandise and supplies introduced into SRA**

The Airport Operator must establish procedures to ensure that all merchandise and supply introduced into the SRA must be subjected to appropriate security controls including supply chain security process or screening.

Stores and supplies intended for carriage on passenger flights (i.e. in-flight supplies), airport supplies may provide a means to introduce prohibited items inside the SRA of airports and on board an aircraft.

Appropriate security controls including supply chain security process which may include screening must be applied to in-flight supplies, must be implemented to ensure that such supplies do not conceal prohibited items that could endanger the safety and security of passengers, crew and aircraft and introduced into SRA.

Airport supplies intended to be used, sold or otherwise made available inside the SRA, and identified as such, include, inter alia:

- (a) consumer goods used or sold in the SRA (e.g. items used or sold at restaurants, gift shops, duty-free stores, offices and airline lounges);
- (b) tools and equipment used for construction work or maintenance of airport structure and services; and
- (c) equipment and parts used for aircraft maintenance or operation (including kerosene/fuel).

**Applicability**

The supply chain of goods necessary for airport operations may include many suppliers. These suppliers provide a wide range of items to airport operators, airport tenants and aircraft operators. The security measures and controls detailed in this chapter should be applied:

- (a) upon entering the SRA if no other form of security controls like a secure supply chain process or screening was applied (and the supplies were not protected thereafter against unauthorized interference);
- (b) in facilities where consolidation of supplies intended for airport use is carried out. Such facilities are usually located StreetSide, including the landside of airports. Security controls, which may include screening, should be applied to airport supplies at such facilities and upon entering the SRA; and
- (c) during the transportation of secured supplies throughout the secure supply chain until entry into the SRA.

Items carried by airport personnel, including maintenance staff, are not considered as airport supplies.

**107.53(d)(20) Procedures for unidentified baggage and suspicious in a accordance with a risk assessment**

The Airport Operator must establish procedures to deal with unidentified baggage and suspicious objects in accordance with a risk assessment.

**107.53( e)(1) Security Designated Airport Barrier Protection**

The holder of an Airport Operating Certificate must develop procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of paragraph (b) are complied with.

**107.53( e)(2) Control and Monitoring of Landside Threats**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the landside areas are controlled and monitored to minimize any threat, including **Management of Vehicular Traffic on Public Roadways in Front of Terminal Buildings, including Unattended Vehicles:**

**(i) vehicle management and speed control:**

- (a) the design, location and features of vehicle access roads and parking areas located in front of terminal buildings should allow for effective control of traffic flow. This should include:
  - (1) the physical separation of public transport vehicles (i.e. taxis and buses) and private vehicles; and
  - (2) the establishment of vehicle management processes that efficiently control access by certain types of vehicles, such as commercial delivery trucks, to certain landside areas;
- (b) security barriers and/or fabricated or natural chicanes should be used to control the speed of vehicles, thereby limiting the capacity for damage through ramming a building. For example, placing obstacles on access roads to terminal buildings, effectively creating an artificial chicane, may help channel vehicle flow to prevent excessive speed.
- (c) appropriate monitoring mechanisms for vehicle entrance should be established so as to not cause queues that could obstruct regular traffic flow, or block road systems in the event of an emergency evacuation. Similarly, rejection lanes should be considered to prevent vehicle build-up
- (d) if car parking areas are located adjacent to terminal buildings, critical infrastructure and aprons, surveillance activities and patrolling regimes should be implemented. For example, the presence of unattended vehicles, or vehicles parked in front of a terminal for an excessive period of time, should be monitored and vehicles removed, in order to minimize the threat posed by VBIEDs (Vehicle Borne Improvised Explosive Devices);

**(ii) management of unattended items in public areas**

the issuance or publicizing of instructions to the general public about the importance of notifying any suspicious activities and/or items to local authorities must be adopted. For example, using posters and/or making public announcements may help raise awareness

among both passengers and non-passengers, and further assist in the detection of suspicious activities and/or unattended items in landside areas of airports.

**(iii) provision of security awareness public announcements**

- communication systems, surveillance systems and security lighting should be deployed for landside areas, to assist patrols in their duty. Security lighting is essential and must be installed on all vehicle routes, perimeters and terminal forecourts;
- appropriate security measures for the landside areas of aviation facilities other than passenger terminals should ensure that the movement of people and goods are constantly monitored (e.g. through the use of CCTV systems) to prevent unauthorised access and identify possible intruders; and

**107.53( e)(3) Prevent Inadvertent Unauthorised Access**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.53(c) and (d) are complied with in relation to safeguards to prevent inadvertent unauthorised access and to deter intentional unauthorised access to any secure area within the Airport, including:

**(i) details of the barrier(s)**

Fences between the landside and airside should be physical obstructions that are clearly visible to the general public and deny unauthorised access. Fencing should be of sufficient height to deter scaling. A minimum height of 2.44 m or 8 ft is recommended, augmented by inclined barbed wire or razor-taped wire. The installation of a fence should prevent a person from pulling it up at the bottom and crawling or burrowing under. Fences may be buried into the ground or affixed to a concrete base or sill. There may be legal implications if barbed or razor-taped wires are used in areas to which the public has access, and legal advice on the matter should be sought.

**(ii) details of access points**

Access control points

All doors, stairs and passenger loading bridges giving access to an apron or to parked aircraft should be locked when not in use. Those doors that are required for use as emergency exits and which are not continually supervised should be equipped with audible alarms and a surveillance system that can be monitored from a location such as an airport security operations control center. The use of frangible devices or covers over emergency exit activation bars may also deter misuse.

Additionally, emergency exit doors should be equipped with a timed-release activation bar, delaying their opening for some five to ten seconds, in order to ensure that once an emergency door alarm is set off, there should be time to attract the attention of security personnel in the vicinity. All electronically controlled locks should “fail safe” in case of a power failure. This means that locks, particularly those on doors serving as emergency exits would automatically unlock if the power is cut.

To prevent the introduction of unauthorised items into the hold baggage handling system, baggage conveyor belts should be protected with access control measures extending from the check-in counter to the airside baggage processing and handling area. Only authorised personnel should be allowed access to the baggage system.

Members of the public and passengers should not be allowed to enter the Airside and Security Restricted Areas respectively, in order to meet arriving passengers at a gate. On entering a Security Restricted Area:

- (a) passengers should be required to produce a valid boarding pass or equivalent in conjunction with a government issued identity document bearing a photograph, such as a passport; and
- (b) all other persons should be required to produce a valid identification permit.

Very Important Person (VIP) facilities require careful consideration, as the individuals using them may be subject to a higher level of personal threat. Facilities should allow for the control of VIPs and those involved with their reception or departure, and should incorporate a dedicated screening area, separate from normal passenger operations, for the check-in and processing of VIP passengers.

If VIP facilities straddle the landside and airside boundary, the standard of access control should be no less than at other access points, and arrangements for the use of these facilities should ensure the integrity of the airside boundary. VIP facilities must be secured when not in use.

**External Access Control Points should incorporate the following design features:**

- (a) an unobstructed view of the surrounding area and easy access and egress for guards to carry out their duties;
- (b) guard accommodation should be weatherproof and ventilated to a standard dictated by the local climate to ensure guards can carry out their duties in all weather conditions. Suitable domestic facilities should be provided;
- (c) if the access control point is used in darkness, lighting should be sufficient to illuminate the gate area and surrounding fence area and should be deployed to assist guards in surveillance of the area;
- (d) the access control point should be situated inside the fence line, along with vehicle control barriers, so that when access gates are closed the access control point is secure and the outside area is clear of objects which could aid an intruder to scale the gates or fence;
- (e) gates, even if drop-arm barriers are used to control vehicle entry;
- (f) hinges which prevent the removal of the gate by lifting, as well as the capability of being locked and of opening outwards;
- (g) suitable communications should be provided to the central security control and, if necessary, the local police authority. Depending on the remoteness of the post, emergency

audible and visual alarms may be required to allow the access point security force to summon assistance;

- (h) if screening is part of the access control measures, an airlock principle should be used to ensure that pedestrians and vehicle occupants are controlled and kept separate from unscreened persons and vehicles;
- (i) if drop-arm barriers are used to control traffic, the access control system should be designed so that pedestrians cannot bypass access control procedures while vehicles are being inspected; and
- (j) if necessary in high-traffic situations, separate access and exit lanes should be constructed, each with its own barriers and gates to ensure the efficient operation of the access control point.

**(iii) details of locking or control system(s), including control of any duct, drain or tunnel giving access to a security area**

If underground service ducts, sewers and tunnels cross the airside or security restricted area perimeter, entrances to all ducts and manhole covers through which access to airside areas is possible should be secured and periodically inspected or protected by intrusion detection devices.

**107.53( e)(4) Security Services Airport Identity Card Procedure**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.53 (e)(11) are complied with in relation to the security of services.

**107.53( e)(5) Cyber Security Procedures for Airport Development**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.53 (e)(12) are complied with in relation to cyber security

**107.53( e)(6) Access Control Procedures**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which he requirements of rule 107.55 are complied with in relation to access control

**107.53( e)(7) Screening Procedures**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.57 are complied with in relation to screening

**107.53( e)(8) Training Programme**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.59 are complied with in relation to the security training programme

**107.53( e)(9) Procedures for Incident Notification**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.61 are complied with in relation to incident notification.

**107.53( e)(10) procedures for Liaison with Other Organisations**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.63 are complied with in relation to liaison with other organisations

**107.53( e)(11) Airport Identity Card Procedure**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.65 are complied with in relation to airport identity cards

**107.53( e)(12) Procedures for Airport Development**

The Airport Operator must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 107.67 are complied with in relation to Airport development;

**107.53( e)(13) Procedures Airport Emergency Plan – Security Related Events**

The Airport Operator must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which the requirements of rule 139.103 are complied with in relation to testing of the Airport Emergency Plan, including the exercising of security related events

Airport Operators, in accordance with their certification requirements under CAR Part 139 are required to develop an Airport Emergency Program (AEP). It is a requirement that the AEP is regularly tested to ensure its effectiveness. This Rule requires the Airport Operators to include or design/develop drills and exercises that consider security related incidents and event and tested on regular basis.

**107.53( e)(14) Procedures to Minimize Unlawful Interference**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which danger to passengers, crew, and ground personnel is minimised if a hijacking, bomb threat, or any other threat or event of unlawful interference occurs

**107.53( e)(15) Procedure for Increased Level of Security Risk**

The holder of an Airport Operating Certificate must establish procedures to ensure that the security measures and procedures required by paragraph (107.53(a) must set out the means by which temporary additional security measures will be implemented to upgrade the security of the Airport if the Director finds or suspects an increased level of security risk to a person on an aircraft, or to an aircraft or an Airport and requires the additional security measures.



## **107.55 Access Control**

### **107.55(1) Insecure Door, Gates and Barriers of Access Control**

The holder of an Airport Operating Certificate for a Security Designated Airport must develop and implement procedures to ensure that no person at a security designate Airport shall, without lawful authority leave open or insecure or otherwise uncontrolled any door, gate or other barrier provided to control access to any security area, enhanced security area or operational area.

All doors, stairs and passenger loading bridges giving access to an apron or to parked aircraft shall be locked when not in use. Those doors that are required for use as emergency exits and which are not continually supervised should be equipped with audible alarms and a surveillance system that can be monitored from a location such as an airport security operations control center. The use of frangible devices or covers over emergency exit activation bars may also deter misuse.

Additionally, emergency exit doors should be equipped with a timed-release activation bar, delaying their opening for some five to ten seconds, in order to ensure that once an emergency door alarm is set off, there should be time to attract the attention of security personnel in the vicinity. All electronically controlled locks should “fail safe” in case of a power failure. This means that locks, particularly those on doors serving as emergency exits would automatically unlock if the power is cut.

### **107.55(2) Measures for Articles Capable of Facilitating the Evasion of Control Measures.**

Tholder of an Airport Operating Certificate for a security designated Airport must develop and implement procedures to ensure that no person at a security designate Airport shall, without lawful authority deposit, or leave adjacent to, or on any fence, barrier, or other thing being used to prevent unauthorized access to any security area, enhanced security area or operational area any article that is capable of facilitating the evasion of control measures.

Where the Airport Operator leases a facility or area or allows any activities to occur which require access to the secure area of the Airport, it is imperative that the third party be required to enter into an agreement ensuring that they indicate their knowledge and understanding that they must ensure that no unauthorised access to the secure area is possible through the area they control. This may be achieved through a contractual clause or a MoU and should be monitored on a regular basis by Airport security officers to ensure ongoing compliance.

## **107.57 Screening**

### **107.57(a)(1) Authority to Conduct Screening**

The holder of an Airport Operating Certificate shall establish procedures to ensure the screening of passengers, crew and baggage, prior to boarding an aircraft, at a security designated Airport is conducted by the Aviation Security Service, or the holder of an aviation security service certificate issued in accordance with Part 140;

- (i) where that function is contracted out to a security service provider, there must be means of ensuring that the contractor complies with the Part 140 certificate holder’s exposition. Where the Airport Operator is the holder of the Part 140 certificate and a contracted third party security company is employed to undertake the screening function, it is imperative that the Airport Operator is able to demonstrate that the contracted service provider has

been provided with the relevant sections of their approved exposition to ensure that it can be complied with at all times.

- (ii) where that function is contracted out to a security service provider, the means of ensuring compliance with the details of any work that is intended to be contracted out to any other organization, the contractual provisions by which the holder of an Airport operator certificate ensures that any such contractor or other agent complies with the requirements of the applicant's Airport Security Programme.

#### **107.57(a)(2) Screening of Passenger, Crew Member and Baggage for Aircrafts Operation from or within Papua New Guinea.**

Each Airport Security Programme shall have procedures to ensure the screening of passengers, crew and baggage, prior to boarding an aircraft, at a Security Designated Airport is conducted by means that ensure compliance with the requirements of rule 108.63(1)

#### **107.57(b) Screening of Non-Passengers, Vehicle and Goods**

Each Airport Security Programme shall have a procedure to ensure the screening of non-passengers, vehicles and goods being taken into designated security areas or enhanced security areas of Airports must be conducted;

- (i) based on a security risk assessment conducted by the Airport Operator.
- (ii) Vehicles and items carried within the vehicle shall be subjected to screening or other appropriate security controls before entering a Security Restricted Area, in accordance with a security risk assessment carried out by the relevant national authorities.
- (iii) in accordance with any direction issued by the Minister under Section 149A of the Civil Aviation Act
- (iv) in accordance with any direction issued by the Director under Section 149B of the Civil Aviation Act.

#### **107.59 Training of Personnel**

##### **107.59(a)(1) Training Programme**

The holder of an Airport Operating Certificate issued for a security designated Airport must establish a security training programme and procedures for ensuring that every person who is employed, engaged, or contracted by the certificate holder has the appropriate level of security awareness applicable to the person's function and those with security responsibilities.

Information related to the specific training requirements for Part 140 Certificate Holders is contained within that Rule Part 140 A.24 and should be incorporated into the Airport training programme. Additional training needs, specific to each Airport must be developed to ensure that all staff with security responsibilities have an in-depth understanding of their roles and responsibilities. Training programmes should be specific to the unique operating environment of the Airport the training relates to.

It should also be noted that it is a requirement that aviation security instructors be suitably certified to deliver training. Additional information in relation to the certification of instructors is contained within the National Civil Aviation Security Training Programme.

**107.59(a)(2) Initial and Recurrent Training**

The holder of an Airport Operating Certificate issued for a Security Designated Airport must establish a procedure to ensure that all personnel involved with or responsible for the implementation of various aspects of the security controls and those authorised to have unescorted access to airside areas must receive initial and recurrent security awareness training containing applicable segments of the following:

- (i) access control to airside areas and security restricted areas;
- (ii) screening of persons other than passengers, together; with items carried, prior to entry into airport security restricted areas;
- (iii) security checks and searches of originating aircraft and protection of the aircraft until departure;
- (iv) measures to identify and manage unruly or disruptive passenger situations;
- (v) measures to protect screened passengers and their cabin baggage from unauthorized interference, including transit passengers and their cabin baggage, and measures to protect the integrity of the security of the airport of transit;
- (vi) screening of hold baggage;
- (vii) measures to protect screened hold baggage from unauthorized interference;
- (viii) hold baggage reconciliation and authorization of hold baggage for carriage;
- (ix) screening of cargo and mail;
- (x) measures to protect cargo and mail subjected to screening or other security controls from unauthorized interference;
- (xi) security controls for catering, stores and supplies intended for carriage on commercial flights, and supply chain security process, if applicable;
- (xii) security controls for merchandise and supplies introduced into security restricted areas, including supply chain security process, if applicable; and
- (xiii) security measures for landside areas.

**107.59(a)(3) Maintenance of Training Records**

The holder of an Airport Operating Certificate issued for a security designated Airport must establish a procedure to ensure that persons implementing security controls possess all competencies required to perform their duties and are appropriately selected and trained according to the requirements of the PNG National Civil Aviation Security Programme (NCASP) and that appropriate records are maintained and up-to-date

**107.59(a)(4) Standard of Performance for Initial and Periodic Assessments**

The holder of an Airport Operating Certificate issued for a security designated Airport must establish a procedure to ensure that relevant standards of performance for initial and periodic assessments must be introduced, implemented and maintained

**107.59(a)(5) Assessment for Competencies for Initial and Recurrent Training**

The holder of an Airport-Operating Certificate issued for a Security Designated Airport must establish a procedure to ensure that all aviation Security Training Programmes for persons with responsibilities under the national civil aviation security programme to include an assessment of competencies to be acquired and maintained for initial and recurrent Training

**107.59(b)(1) Applicable Segments for Initial and Recurrent Training**

The holder of an Airport Operating Certificate must establish training programme required by paragraph (a) must contain applicable segments for initial training and recurrent training

**107.59(b)(2) Knowledge Testing or Competency Assessment**

The holder of an Airport Operating Certificate to establish the training programme required by paragraph (a) must contain knowledge testing or competency assessment as appropriate for the training conducted

**107.59(c )(1) Training Syllabus**

The holder of an Airport Operating Certificate issued for a security designated Airport must ensure that each segment required by paragraph (b)(1) includes a syllabus that is acceptable to the Director.

**107.59(c )(2) Authorisation to conduct training**

The holder of an Airport Operating Certificate issued for a security designated Airport must ensure that each segment required by paragraph (b)(1) is conducted in a structured and coordinated manner and carried out by the holder of an aviation training organization certificate issued under Part 141 that authorizes the conduct of such a course

**107.59(c )(3) Instructor qualification and Certification**

The holder of an Airport Operating Certificate issued for a security designated Airport must ensure that each segment required by paragraph (b)(1) includes the development and implementation of a certification system to ensure that instructors are qualified in the applicable subject matters in accordance with the National Civil Aviation Security Programme (NCASP).

**107.59(d ) Recurrent Training Interval**

The holder of an Airport Operating Certificate issued for a security designated Airport must establish process to ensure that every person who is required to be trained undertakes the recurrent training segment of the training programme at an interval of not more than 2 years.

**107.59(e)(1) Records of Persons Authorized to Conduct Training**

The holder of an Airport Operating Certificate issued for a Security Designated Airport must establish procedures to ensure that there is a record of every person who conducts a security training segment under the authority of the certificate.

**107.59(e)(2) Records of Persons Undertaking Security Training**

The holder of an Airport Operating Certificate issued for a Security Designated Airport must establish procedures to ensure that there is a record of every person who undertakes security training conducted under the authority of the certificate

**107.59(f)(1) Record of Name of Persons Attending Training**

The holder of an Airport Operating Certificate must establish procedures to ensure that the records required by paragraph (e)(1) must include name of the person conducting training.

**107.59(f)(2) Record of Instructor Competencies, Experience and Qualifications.**

The holder of an Airport Operating Certificate must establish procedures to ensure that the records required by paragraph (e)(1) must include details of the training, competencies, or experience that qualifies the person to conduct the training.

**107.59(f)(3) Record of Scope of Training**

The holder of an Airport Operating Certificate must establish procedures to ensure that the records required by paragraph (e)(1) must include the scope of training that the person may conduct.

**107.59(g)(1) Record of Name and Date of Birth of Person Conducting Training**

The holder of an Airport Operating Certificate must establish procedures to ensure that the records required by paragraph (e)(2) must include the name and date of birth of the person who undertakes training.

**107.59(g)(2) Record of the Identity of the Training Segment**

The holder of an Airport Operating Certificate must establish procedures to ensure that the records required by paragraph (e)(2) must include the identity of the training segment.

**107.59(g)(3) Record of Attendance, Instructor Comments, Test Results and Assessments**

The holder of an Airport Operating Certificate must establish procedures to ensure that the records required by paragraph (e)(2) must include details of the person's attendance, instructor comments, and the results of tests or assessments, as applicable

**107.59(h)(1) Accurate, Legible and Permanent Nature Records**

The holder of an Airport Operating Certificate must establish procedures to ensure that the records required by paragraph (e) must be accurate, legible and of a permanent nature

**107.59(h)(2) Record Retention Period**

The holder of an Airport Operating Certificate must establish procedures to ensure that the records required by paragraph (e) must be retained for a period of 3 years from the date of the last entry.

**107.61 Incident Notification and Reporting****107.61(1) Incident notification are complied with requirements of rule Part 12**

Each Airport Security Programme is required to establish a procedure to ensure the requirements of Part 12 are complied with in relation to notifying, and where applicable reporting to the Director, any security incident involving the Airport.

**107.61(2) Incident Notification Liaison with Other Organization**

Each Airport Security Programme shall have a procedure to ensure the requirements of rule 107.53(e)(10) are complied with in relation to, breaches of and deficiencies in, security procedures.

## **107.63 Liaison with Other Organizations**

### **107.63(a)(1) Liaison and Consultation with Other Organization involved in Contingency Planning.**

The holder of an Airport Operating Certificate issued for a Security Designated Airport must, for each Security Designated Airport it operates, establish a process to consult and liaise with all other organizations involved in contingency planning affecting the security of operations at that location

### **107.63(a)(2) Establishing Airport Security Committee**

The holder of an Airport Operating Certificate issued for a Security Designated Airport must, for each Security Designated Airport it operates establish a security committee to ensure that sufficient information is given to other organizations at that location to motivate security awareness on the part of all personnel.

The establishment of a Security Committee is an essential element in the achievement of aviation security outcomes. Membership of the committee should be representative of stakeholders and should be attended by persons with specific security knowledge/responsibility and/or sufficient authority to make decisions on behalf of their organization. Minutes of meetings should be provided to the National Civil Aviation Security Committee to support high-level decisions on legislation and policy settings.

## **107.65 Airport Identity Cards**

### **107.65 (a) Directors Approval for Issue of Airport Identity**

The operator of an Airport Operating Certificate is required to establish policies and procedures as subjected to the approval of the Director.

### **107.65(b)(1) Background checks**

The holder of an Airport Operating Certificate must establish a procedure that all applications for the issue of an Airport Identity Card should be supported by a verification letter or the approval of the individual's employer. Airport Identity Cards are a means of ensuring only people with a need have access to secure areas and this is supplemented by a background check of the applicant.

The background check may include some or all of the following:

- birth records or confirmation of identity
- criminal history checks completed by the Police,
- employment history,
- residential history,
- visa (right to work) check

Ultimately, it is the responsibility of the issuing authority to satisfy themselves that the person is who they say they are and that their employment creates a legitimate need for them to have access to secure areas at the airport. Access control should however be restricted to only those secure areas that the person requires to access in the normal course of their duties.

The card itself should have a clear photo of the applicant (no sunglasses, hats etc.) and include additional information, such as:

- name of the applicant (unless the Director consents to concealing that information for security reasons),
- name of the applicant's employer,
- expiry date of the card,
- if zones have been established at the airport, which zones the card holder may access,
- the applicant's signature

All permits shall be issued by the holder of an Airport Operating Certificate, normally the airport security section, and within the policy guidelines issued by CASAPNG Avsec Branch. Strict control and accounting procedures should be established and maintained. The use of a computer database for tracking the issuance and control of permits may be invaluable. Such a system provides the basis for the efficient administration of an access control system, and additional benefits in relation to lost or stolen permits or permit cancellation procedures.

At larger Airports (including Port Moresby International Airports), consideration should be given to the division of Security Restricted Areas into zones based on the functions normally carried out in those areas, with corresponding annotations on the permits. Permits should indicate by means of numerical, alphabetical or colour-coding the zones a particular person is authorized to access. Access into specific areas should only be granted on a need-to-go basis for the purpose of carrying out official duties. For example, employees who require access to maintenance hangars may not need to access the aircraft parking apron, in which case their permits should indicate permission to enter only the maintenance zone.

Applications for individual permits must be initiated by the employer in writing, supplying full personal details and job descriptions, as well as a reason for the employee's need for access. Strict precautions must be taken to avoid issuing permits to employees who do not need, or rarely need, to enter security restricted areas. The job position or title should not be used as the criterion for establishing the need for a permit.

Persons requiring a permit should be obliged to collect it personally, in order that the photograph and signature and other personal features such as personal identification numbers may be verified. The recipient should be acquainted with the conditions of issuance and should sign a certificate to that effect.

It is inevitable that, on occasion, permits will be lost. The loss or theft of a permit should be reported immediately in person, by telephone and in writing to the sponsor and to the issuing authority. The issuing authority should have a system in place to notify all concerned that the permit is no longer valid, and this notification should be issued immediately or as soon as possible on receipt of the loss or theft report.

Losses shall be recorded and documented by the issuing authority. When the nature or number of losses of unexpired permits is such that the credibility of the permit system in its entirety is undermined, the current issuance of permits should be withdrawn and replaced, system wide, by a new one, preferably bearing a new design or layout.

### Background checks

A background check to confirm a person's identity and previous work experience, including criminal history when legally permissible, whenever appropriate, shall be carried out as part of the assessment of the individual's suitability for unescorted access to airside and security

restricted areas. Background checks shall be updated on a regular basis to ensure that the individual still meets the required criteria. A good practice is to update a background check every time airport security identification permits need to be renewed.

Background checks must be supported by a legal framework that establishes general criteria, including the right to appeal a negative decision about a person's suitability to enter a security restricted area without escort. Such criteria should also include verification of an applicant's:

- (a) identity, by means of a passport or national identity card or the records of registry of birth, national insurance number, etc.;
- (b) trustworthiness and capacity to work unescorted within a security restricted area, by means of a check of criminal history and, depending on the specific function to be performed, other personal circumstances or behavior that could forewarn of danger; and
- (c) place of residence during the previous five years, or another period determined by the State's legislation or the appropriate authority, and the dates, names, telephone numbers and addresses of previous employers or schools attended during this period, with explanations for any gaps in employment of more than one month.

Provisions regarding foreign nationals and national citizens who have lived abroad requesting issuance of an identification permit to access security restricted areas should be established, in order to ensure that applicants have not been convicted of a disqualifying offence in their State of origin.

Background checks may only review lawfully accessible information. Furthermore, prior to conducting a background check, written consent should be obtained from the permit applicant. At the same time, it should be made clear to the applicant that failure to give consent to a background check will result in rejection of the application.

All companies and organizations at an airport should vouch for the valid requirement for each permit prior to its issuance to an employee. It is the employer's responsibility to complete adequate pre-employment checks or other inquiries to ensure that the individual concerned does not pose a potential threat to the airport. Permits shall not be issued without such guarantees.

A permit shall not be issued if, during the performance of a background check, it is determined that the applicant was convicted of:

- (a) certain crimes, specifically possession or use of illicit drugs, trafficking in illicit drugs, trafficking in weapons or illegal possession of weapons, aggravated assault, extortion, acts endangering public safety including acts of unlawful interference against civil aviation, sexually-related offences or membership in a criminal organization. In exceptional circumstances, the national authority may determine that the applicant has been fully rehabilitated and no longer constitutes a risk
- (b) other relevant offences such as burglary, dealing of stolen goods, embezzlement, fraud and fraudulent misrepresentation, without making restitution.



Applicants for jobs implementing security controls should undergo a supplementary check to confirm that they are not associated with a terrorist organization. Generally, these duties involve controlling access to and searching security restricted areas and aircraft, issuing identification permits to persons or for vehicles, or managing any persons performing these functions.

#### **107.65(b)(2) Recurrent Background Checks**

Subjected to Paragraph (c) the holder of an Airport Operating certificate must establish a procedure that an airport identity card may be issued only if the person applying for the airport identity card has completed the following background check of the recurrent background checks are applied to such persons at an interval of not more than 2 years.

In order to reduce the possibility of misuse, permits should have a defined period of validity that should not exceed two years. Permit renewal should adhere to a schedule based on the number of renewals required, and the process should allow sufficient lead time to cater to administration and production needs while ensuring that no permits remain in use after their expiry date. This requirement may pose administrative difficulties for airports with large numbers of workers, unless they establish staggered periods of validity. For example, re-issue may be conducted progressively over a period of time, so that a certain number of permits are due for renewal each month or each quarter.

#### **107.65(b)(3) Persons Found Unsuitable by Background Checks.**

Subjected to Paragraph (c) the holder of an Airport Operating Certificate must establish a procedure that an airport identity card may be issued only if the person applying for the airport identity card has completed the background check. If the persons are found unsuitable by any background check, the person shall be immediately denied the ability to implement security controls, unescorted access to Security Restricted Areas, and access to sensitive aviation security information

##### **Gaps in history**

Gaps in an applicant's personal or employment history are not acceptable except for the usual time allowed for holidays, about one month per year. However, when it is not possible to check the continuous criminal history or experience of an applicant over the defined period, verification of the person's suitability to hold a permit may be sought from alternative sources, such as former employers located abroad or, for a self-employed applicant, the national tax authority or other relevant government authorities.

Responsibility for issuing a permit remains with the permit issuing airport operator, and due care and discretion should be exercised in examining information. Before issuing a permit, the issuing airport operator must be fully satisfied of the applicant's suitability as a holder.

After making every effort to obtain information, if the applicant's identity and previous experience, including criminal history, cannot be verified, the individual shall be regarded as unsuitable for a permit.

#### **107.65(c) Temporary Identity Card**

The holder of an Airport Operating Certificate to establish procedures for temporary identity card. The background check referred to in 107.65(b) is not required if the person making an application for an identity card is issued with a temporary identity card approved by the Director that entitles

the person to enter and remain in a security area or enhanced security area of any security designated Airport or security designated navigation installation when escorted by a person issued with an airport identity card in accordance with the background check process referred to in 107.67(b).

During periods of increased threat levels or a specific threat, it may be necessary to boost the existing identification permit system with special temporary permits or cards that are issued daily to authorize personnel and retrieved at the end of their duty shifts. In order to assure that temporary permits are not issued for an extended time period, their validity should be limited (e.g. 30 days).

The holder of an Airport Operating Certificate may issue a short-term or temporary permit, on which the period of validity is clearly stated, to each official guest and non-resident professional or technician requiring access to airside or security restricted areas in order to perform assigned tasks. Temporary permits need to incorporate a photograph, and indicate what special equipment the holder is authorized to convey into airside or security restricted areas. Persons requesting temporary permits must provide a government-issued photographic identification such as a passport or driver's license, as well as proper accreditations before being issued the temporary permit.

All temporary permits must be recovered by the issuing authority, with adequate records being maintained to facilitate this process and provide for protection against misuse. The security of unissued temporary permits is also important, and stock should be strictly controlled and held under secure conditions.

### **Visitor escorts**

All visitors to airside and security restricted areas shall be escorted, and be issued a one-day visitor permit clearly indicating the identity of the escort. When the volume of visitors at any particular time is expected to exceed the supervisory capacity of airport security services personnel or operational staff, requests for assistance from police, the military or another authority should be considered. Visitor permits need not incorporate a photograph.

The number of visitors who are permitted to be escorted by the holder of an Airport Security Identification Permit shall be well defined in ASPs. This number may vary according to the type of permit issued, the area or zone being visited and the current threat level set by the Director. The number may also depend on the results of security risk assessments carried out by the relevant national authorities with Papua New Guinea.

### **107.65 (d) Authorised Persons for Security Restricted and Security Enhanced Areas**

The holder of an Airport Operating Certificate to establish procedures subject to paragraphs (e) and (i), no person shall enter or remain in any security area or enhanced security area of any security designated Airport or security designated navigation installation, unless that person wears an airport identification card or has on or her possession or other identity document.

#### **107.65(d)(1) Wearing of Airport Identification Card**

The Airport Operator must establish procedures to ensure wearing or displaying of Airport Identity Card on the front of his or her outer garment.

**Wearing of permits**

Permits must be worn or displayed by all staff and visitors within the area for which they are issued. They should be visibly displayed on an outer garment above the waist. In those areas where it is considered necessary for safety purposes, the outer garment should be designed with a transparent pouch into which the permit can be placed and thus securely displayed. The prominent display of permits has the following benefits:

- (a) any individual seen without a permit may be immediately challenged
- (b) visitors or contractors are readily distinguishable from permanent staff.

In certain cases, such as when law enforcement officers undertake covert duties or if personal safety may be at risk, deviations from the requirement to display permits may be allowed by the appropriate authority. Exceptions are clearly defined in the NCASP.

**107.65(d)(2) Another Identity Document**

The Airport Operator is required to establish procedures for possession of another identity document or other identity documents for the time being approved under paragraph (a).

**107.65(e) Holders Name Not Disclosed**

The holder of an Airport Operating Certificate is required to establish procedures where the Director considers it desirable that the name of the holder of an airport identity card be not disclosed, the Director may approve the wearing of an identity card from which the holder's name has been deleted.

**107.65(f) Authorised Persons in Security Area**

The holder of an Airport Operating Certificate is required to establish procedures for a person who is authorized by this rule to enter a security area shall remain in that area only for the purposes of his or her duties.

**107.65(g) Airport Identity Card Inspection**

The holder of an Airport Operating Certificate is required to establish procedures. If required to do so by an authorized person, any person entering or in a security area or security enhanced area shall produce for inspection his or her airport identity card or other identity documents for the time being authorized under paragraph (a).

**107.65(h) Holder of an Airport Identity Card Cease of Employment**

The holder of an Airport Operating Certificate is required to establish procedures if the holder of an airport identity card ceases to be employed in a position for which the card is required, or for any other reason ceases to be entitled to hold the card, the holder shall forthwith return the card to the issuing authority.

It is to be expected that persons ceasing to work at an airport will on occasion leave with their permits. Provision should be made to immediately recover a permit when a holder ceases to need the access it affords, in particular when the term of employment ends or there is a transfer to other duties or locations.

**107.65(i)(1) Crew of Aircraft Engaged in International Operation**

The holder of an Airport Operating Certificate must establish procedures that, nothing in paragraph (b) shall apply to any member of the crew of an aircraft engaged in an international air operation who wears on his or her outer garment an official identity card issued by his or her employer or the government of the state in which he or she permanently resides;

Given the difficulties of control and accounting procedures, it is not appropriate to issue permits to crews of foreign aircraft operators using an airport, even if they use the airport regularly. Provision for the acceptance of their official aircraft operator identification or home State system must be incorporated into security restricted area entry procedures. The airport authority shall ensure that identification documents issued to aircraft crew members conform to the relevant specifications set forth in Machine Readable Travel Documents (Doc 9303). Uniforms alone shall not be considered adequate and sufficient identification.

**107.65(i)(2) Official of a Papua New Guinea Government Agency on Official Duties**

The holder of an Airport Operating Certificate to establish procedures that, nothing in paragraph (b) shall apply to any official of a Papua New Guinea government agency who is required, by reason of his or her official duties, to remain incognito;

**107.65(i)(3) Passengers Entering Security Restricted Areas**

The holder of an Airport Operating Certificate must establish procedures, that nothing in paragraph (b) shall apply to any passenger who enters or leaves a security area for the purpose of joining or leaving a flight, if he or she is in possession of a valid boarding pass for that flight or is being escorted by a crew member or a representative of the operator.

Passengers shall be required to produce a valid boarding pass or equivalent related boarding document in conjunction with a government-issued identity document such as a passport before being allowed to enter an airside or security restricted area and prior to boarding an aircraft. Members of the public shall not be allowed to enter airside or security restricted areas in order to bid farewell to departing passengers or greet arriving passengers, if applicable.

**107.65(i)(4) Pilot In Command of Aircraft not Engaged in Air Operations**

The holder of an Airport Operating Certificate must establish procedures, that nothing in paragraph (b) shall apply to any pilot-in-command of an aircraft engaged in operations that are not air operations who enters or is within a security area for the purpose of embarking, disembarking, or servicing the aircraft, if the pilot has in his or her possession a valid pilot license, or any person being escorted by that pilot.

**107.65(j) Updating Security Features and Design of Approved Airport Identification Card**

The holder of an Airport Operating Certificate must establish procedures for updating the security features and design of the approved airport identification cards at the interval of not more 12 months.

**Permit design**

The most widely used identification permit systems rely on visual inspections of permits by guards at access control points. Permits must clearly display the essential information required by the

control point officer in order to establish the bona fides of the permit holder. To facilitate visual inspection, permits should be designed for display in a prominent position on the holder's outer garment.

There are significant security advantages in adopting permits that include a photograph of the holder, mainly because this acts as a deterrent against unauthorised use by another individual. Photographs should be taken against a contrasting backdrop, with the face photographed in maximum close-up and occupying at least one-third of the permit's dimensions. For convenience and ease of inspection, permits should be 85 mm x 55 mm, that is, about credit card size. Permit designs must incorporate the following features:

- (a) forgery prevention achieved by using a complicated background or fine-line design. The background part of the obverse(opposite) of a permit that is not occupied by the photograph. A guilloche is a continuous geometric pattern over the entire obverse of a permit, including the photograph;
- (b) aid recognition achieved by using a bold overall motif printed over the background; and
- (c) an effective lamination process and the use of security printing on the surface of the laminate that is only visible when viewed at an oblique angle, thus impeding photo substitution.

The obverse (front) of a permit should contain, at a minimum, the following information:

- (a) expiry date clearly stating numerically the month and year of expiry of the permit, preferably in a different colour to highlight the information. This date is the key visual feature in ensuring that expired permits can be discerned when challenged and are not used to gain access;
- (b) security restricted areas for which the permit is valid, authorising the holder to enter them;
- (c) the name of the holder. This must be verified against another form of identification, such as a passport, driver's licence or identification card, if necessary;
- (d) the name of the employer; and
- (e) the permit's serial number, along with, if necessary, the name of the employer, to assist administrative staff in the maintenance of permit records

### **107.67 Airport Development**

It is imperative that aviation security be considered at the point of conception for any proposed Airport developments to ensure that any changes to the Airport layout or usage do not create security vulnerabilities or restrict the potential need to upgrade security requirements in the future. Airport developments should be a standing agenda item for airport security committee meetings to enable stakeholders to value add to the proposal development stage.

Each Airport security programme must establish procedures to ensure that aviation security requirements are met prior to approval to undertake any Airport development that is within or adjacent to the Airport boundary or will be directly impact upon any designated security areas, enhanced security or sterile areas.

## **107.69 Vehicle Passes**

### **107.69(1) Vehicle Permit System**

The holder of an Airport Operating Certificate to establish procedures for a vehicle permit system

#### **Vehicle permits**

The admittance of non-service vehicles to airside areas shall be restricted for security and operational reasons to avoid congestion on aircraft parking aprons and since, for example, an unlawful act may be materially assisted by the use of a vehicle, both for gaining access quickly to an aircraft or facility, and for leaving the scene. The control of vehicular access to the airside therefore serves as a preventive measure.

Access to airside or security restricted areas on a continuing basis shall only be granted to those vehicles that have a regular requirement for such access. Such vehicles should also ideally remain airside when not in use, thus minimizing vehicular traffic at access control points.

Provisions should be made for vehicles that require infrequent access to airside and security restricted areas, for example vehicles carrying oversized cargo directly to an aircraft or making deliveries to airside maintenance contractors and construction sites. Vehicle permits for such vehicles should be clearly distinguishable from permits allowing access on a continual basis.

At larger airports, it may be necessary to issue vehicle permits for specific security zones, in a manner similar to the issuance of employee permits. Vehicle operators should be required to fully justify the operational need for entry to airside and security restricted areas.

No vehicle permit should be issued until evidence of appropriate insurance coverage has been produced.

Vehicle permits should be issued for a fixed term only, and for a period that does not exceed one year. Permits should not be transferable from one vehicle to another. Permits should be verified on every occasion before a vehicle enters or leaves a security restricted area and should be subject to oversight activities.

When a higher level of security is required, vehicle permits should be issued as vehicles enter the airport, and retrieved at the time of their departure.

Vehicle permits should only be issued to vehicles on a need-to-access basis, on receipt and approval of written applications, and shall contain the following information:

- (a) period of validity, to a maximum of 12 months;
- (b) security restricted areas for which the permit is valid, if applicable;
- (c) access control points that the vehicle is allowed to use;
- (d) name of vehicle owner and/or operator; and
- (e) vehicle registration index or serial number.

Vehicle permits must be affixed to and permanently displayed on the front of the vehicle for which they are issued. They shall be clearly visible when the vehicle is entering Security Restricted Areas and should be of a design that is difficult to remove, alter or forge.

The fact that a vehicle displays a valid permit must not be taken to imply that the vehicle's occupants have authorized access. The identification documents and personnel permits of all occupants must be checked before permitting access for the vehicle.

All vehicles that operate on the airside must be immobilized or safeguarded when not in use. Such vehicles should be carefully searched after being left unattended for any period of time to ensure that no restricted articles have been concealed in them. This is particularly important for vehicles parked outside a Security Restricted Area and used to bring equipment or provisions to an aircraft.

### **107.69(2) Period Renewal of Vehicles Passes**

The holder of an Airport Operating Certificate to establish procedures for the periodic renewal of vehicle passes at intervals of not more than 12 months.

### **Permit holder briefings Additional guidance information**

A permit holder should be given a briefing on airport security as a condition for access to airside, security restricted areas and other controlled areas or installations.

The issuing authority should be responsible for ensuring that permit holders receive the requisite briefing before granting access to airside and Security Restricted Areas. If the issuing authority has established that an aircraft operator or other agency is authorised to provide an appropriate briefing to its own employees, it may delegate this task to the employer. Otherwise, the issuing authority itself should arrange for the briefings. The quality of briefings given by another party should be monitored by the issuing authority to ensure that it meets the required standards.

Ideally, the security briefing should be given at the time the staff member receives a permit. If an adequate briefing is not practicable at the time of issuance, it may be given during induction training, provided this occurs within one month, and before the individual is allowed to enter airside and security restricted areas.

Security briefings may be conducted in a variety of ways, and the issuing authority may select the means that most effectively communicate the content and suit local circumstances. Briefings may be given orally, through a video or on a printed handout, and may form part of an employee's aviation security awareness training. A simple test should be incorporated, to confirm that the permit recipient has understood the content and language.

Security briefings should elaborate on the purpose and validity of permits, and describe the holder's responsibilities. In brief, permit holders should be familiar with permit regulations and comply with them at all times, and should be made aware that:

- (a) the permit is to be used by the person to whom it was issued when carrying out authorized company business only, in airside or security restricted areas;
- (b) penalties apply for the misuse of a permit, including withdrawal of the permit by the issuing authority and possible prosecution, in accordance with the laws of the State;

- (c) the aim of airport security is to protect passengers, flight crew, aircraft and airport operator staff and members of the public against acts of unlawful interference with civil aviation;
- (d) they are responsible for safeguarding the permit and held accountable for its use;
- (e) in case of a lost permit, they should report the loss immediately to the issuing authority;
- (f) the permit remains at all times the property of the issuing authority and should be surrendered to the issuing authority when its validity has expired or the need for access no longer exists;
- (g) the permit should be worn above the waist on the outer garment at all times when in an airside or security restricted area;
- (h) inspection of the permit should be permitted on demand by an appropriate authority such as security staff, police officers, customs and immigration officers, an airport terminal manager and personnel working in a security sensitive area such as a departures gate; and
- (i) it is unlawful for any person at an airport to have any restricted article such as a firearm, or object resembling a firearm, or explosives without lawful authority and a legitimate reason to do so.

Additionally, a permit holder is expected to uphold Airport Security by:

- (a) complying with access control regulations and maintaining security measures in his or her work area;
- (b) strictly abiding by the escort rules of the issuing authority; and
- (c) reporting to security staff or control authorities:
  - (i) any breach of access control procedures;
  - (ii) the presence of firearms, other weapons or explosive devices;
  - (iii) the presence of unaccompanied baggage in public places; and
  - (iv) any situation or incident that could represent a security risk, which arouses suspicion, or which may compromise the safety and security of civil aviation.

A record should be kept of all persons receiving security briefings. This record should include the names of the persons involved, the positions held by permit recipients, the identities of the employers and the dates of the briefings. Since the need for a staff member to be given a security briefing is linked to the issuance of a permit, it is recommended that the record of permit issuance be used as a record of briefings as well.



## **Subpart C — Transition Provisions**

### **107.101**

Transition provisions detailed in Part 20 apply to this Part

### **APPENDIX A – Model Airport Security Programme**

The following model Airport Security Programme has been provided as a template for consideration in the development of an ASP. There is no obligation to use it however, prompts have been included and should be considered if developing a new or amending an existing programme.

**MODEL**

**AIRPORT SECURITY PROGRAMME  
(SECURITY DESIGNATED AIRPORTS)**

**XX SAMPLE XX**

**AIRPORT SECURITY PROGRAMME**

**PURPOSE**

**XX Sample XX** Airport has regular air operations provided by aircraft with a passenger-seating configuration of 20 seats or more, excluding any required crew member seat, and as such is required to hold a certificate under Civil Aviation Rule Part 139.

It is also a security-designated Airport in accordance with Section 153 of the Civil Aviation Act 2000 (as amended).

The development of this Airport security programme has taken into account the current threat environment and the specific risk profile of civil aviation operations at **XX Sample XX** Airport.

In accordance with the requirements of Civil Aviation Rule Part 139.201(d)(15), this Airport security programme has been developed as a means of capturing the relevant aviation security measures and procedures that have been implemented at **XX Sample XX** Airport to safeguard against an act of unlawful interference with civil aviation. It has been designed to comply with the requirements of the PNG National Civil Aviation Security Program and has been developed in accordance with the guidance contained within the Civil Aviation Rule Part 139 Advisory Circular.

The purpose of this Airport security program is to ensure that appropriate measures and procedures are identified and implemented to minimise the likelihood of an act of unlawful interference occurring. It seeks to ensure a coordinated approach to the achievement of this outcome by promoting a shared understanding of roles and responsibilities between the airport operator and relevant stakeholders, including airlines and airport tenants. As such, this Airport security programme will be shared, in whole or in part (as necessary), on an as needed basis.

This Airport security programme will identify the minimum standards that must be complied with, as detailed in the Civil Aviation Act 2000 (as amended) and relevant Civil Aviation Rules. It is expected that airport users and tenants will incorporate, where appropriate, the stated measures and procedures into their internal security operations to ensure a consistent application across the airport.

**SENIOR PERSON'S STATEMENT**

This Section should include a statement from the most senior person identified in the Part 139 exposition, outlining the organizations approach to the achievement of aviation security outcomes.

The issues addressed in the statement should include...

- importance of aviation security to civil aviation
- organization's commitment to the achievement of aviation security outcomes
- assurance that adequate human and physical resources will be provided
- assurance that adequate training will be provided, including recurrent training

- acknowledge that the threat environment and risk profile were considered in its development
- recognition that the document is subject to regular review and amendment
- requirement that (relevant) aviation security personnel report directly to senior executive
- commitment to internal quality assurance (Civil Aviation Rule Part 100 requirements)

# Table of Contents

## PURPOSE

## SENIOR PERSON'S STATEMENT

### 1. ORGANISATION

#### 1.1. LEGISLATION

- 1.1.1. International Conventions
- 1.1.2. Civil Aviation Act 2000 (as amended)
- 1.1.3. Civil Aviation Rules
- 1.1.4. National Civil Aviation Security Program

#### 1.2. ALLOCATION OF RESPONSIBILITIES

- 1.2.1. Airport Administration
- 1.2.2. Airport Security Manager
- 1.2.3. Aviation Security Service Provider
- 1.2.4. Contracted Security Service Provider
- 1.2.5. Royal Papua New Guinea Constabulary
- 1.2.6. PNG Air Services Limited
- 1.2.7. Aircraft Operators
- 1.2.8. Air Cargo Agents
- 1.2.9. Border Control Authorities
- 1.2.10. Ground Handling Service Providers
- 1.2.11. General Aviation Operators
- 1.2.12. Airport Tenants

#### 1.3. COORDINATION AND COMMUNICATION

- 1.3.1. Airport Security Committee
- 1.3.2. Communication with Stakeholders
- 1.3.3. Management of Classified Information
- 1.3.4. Management of Media Requests

### 2. DESCRIPTION OF AIRPORT

#### 2.1. PHYSICAL CHARACTERISTICS

- 2.1.1. Airport Location
- 2.1.2. Airport Plans
- 2.1.3. Airport Facilities
- 2.1.4. Airport Operations
- 2.1.5.

### **3. AIRPORT SECURITY MEASURES**

#### **3.1. OVERVIEW**

#### **3.2. LANDSIDE SECURITY**

- 3.2.1. Management of Terminal Kerbside and Carparks
- 3.2.2. Management of Unattended Vehicles
- 3.2.3. Management of Terminal Public Areas
- 3.2.4. Management of Unattended Baggage or Items

#### **3.3. AIRSIDE SECURITY**

- 3.3.1. Designation of Security Areas and Enhanced Security Areas
- 3.3.2. Airport Permit System
- 3.3.3. Perimeter Security
- 3.3.4. Access Control
- 3.3.5. Screening of Airport Workers
- 3.3.6. Inspection of Airside Vehicles
- 3.3.7. Escort Procedures
- 3.3.8. Mobile Patrols
- 3.3.9. Key Control System
- 3.3.10. Protection of Aircraft
- 3.3.11. Protection of Baggage Being Moved Around the Airport
- 3.3.12. Protection of Cargo and Mail Being Moved Around the Airport
- 3.3.13. Protection of Navigational Aids and Vital Facilities

#### **3.4. SCREENING REQUIREMENTS**

- 3.4.1. Sterile Areas
- 3.4.2. Screening Equipment
- 3.4.3. Prohibited Items
- 3.4.4. Separation of Screened and Unscreened Persons
- 3.4.5. Sterile Area Breach
- 3.4.6. Screening of Passengers and Crew
- 3.4.7. Screening of Cabin Baggage
- 3.4.8. Screening of Checked Baggage
- 3.4.9. Passenger and Checked Baggage Reconciliation
- 3.4.10. Screening of Goods Taken Into the Sterile Area

### **4. HEIGHTENED THREAT**

#### **4.1 ADDITIONAL SECURITY MATTERS**

## **5. RESPONSE TO ACTS OF UNLAWFUL INTERFERENCE**

### **5.1. ACT OF UNLAWFUL INTERFERENCE**

- 5.1.1 Emergency Operations Centre
- 5.1.2 Bomb Treat
- 5.1.3 Civil Unrest
- 5.1.4 Cyber Security

## **6. TRAINING**

- 6.1.1 Security Awareness
- 6.1.2 Airport Security Staff
- 6.1.3 Contracted Service Providers
- 6.1.4 Screener Certification

## **7. SAFETY AND QUALITY MANAGEMENT SYSTEMS**

## **8. APPENDICES**

## **1. ORGANISATION**

### **1.1. LEGISLATION**

#### **1.1.1. International Conventions**

*(This Section should reference PNG's obligations as a signatory to the Chicago Convention on International Civil Aviation to comply, to the extent possible, with the Standards and Recommended Practices contained within Annex 17 to the Convention).*

#### **1.1.2. Civil Aviation Act 2000 (as amended)**

*(This Section should outline the key aspects of the Civil Aviation Act as they relate to the achievement of aviation security outcomes).*

#### **1.1.3. Civil Aviation Rules**

*(This Section should identify the key Civil Aviation Rule Parts relevant to the development of the Airport Security Program, including Part 139, Part 140, Part 100, Part 108, Part 109 and Part 171).*

#### **1.1.4. National Civil Aviation Security Program**

*(This Section should note that the Airport Security Program has been developed to complement the requirements contained in the National Civil Aviation Security Program).*

## **1.2. ALLOCATION OF RESPONSIBILITIES**

### **1.2.1. Airport Administration**

*(This Section should outline the hierarchy of roles and responsibilities within the airport administration. It would be useful to include an organizational chart here, or as an appendix, to show the relationship between the most senior person with aviation security responsibilities and the senior executive of the organization).*

### **1.2.2. Airport Security Manager**

*(This Section should identify the position responsible for the implementation of the Airport Security Program and the achievement of aviation security outcomes. Note that any reference to a person will require that the program be amended when staff movements occur, so it is preferable to nominate a position).*

### **1.2.3. Aviation Security Service Provider**

*(This Section should include the details of Part 140 certificate holder for the airport. Where more than one Part 140 certificate holder exists, for example an airline holds a certificate specific to their individual operations, in addition to the airport operator, this should be detailed here to provide clarity).*



#### **1.2.4. Contracted Security Service Provider**

*(This Section should contain details, where any security functions are contracted out to a third party, of the contractual provisions that ensures the third party will comply with all of the requirements of this Airport Security Program).*

#### **1.2.5. Royal Papua New Guinea Constabulary**

*(This Section should highlight the role and responsibility of the RPNGC, noting the stated function contained within the Civil Aviation Act).*

#### **1.2.6. PNG Air Services Limited**

*(This Section should highlight the role and responsibility of PNG ASL at the airport. Specific security requirements for PNG ASL should be included in their security program required by Part 172. That document may be referenced here to avoid duplication but it is imperative that agency consult in the development of their programs to ensure there is no conflicting security procedures and measures. Agencies should also make copies of their security programs available to each other).*

#### **1.2.7. Aircraft Operators**

*(This Section should highlight the role and responsibility of aircraft operators at the airport. Specific security requirements for PNG ASL should be included in their security program required by Part 108. That document may be referenced here to avoid duplication but it is imperative that agency consult in the development of their programs to ensure there is no conflicting security procedures and measures. Agencies should also make copies of their security programs available to each other).*

#### **1.2.8. Air Cargo Agents**

*(This Section should highlight the role and responsibility of air cargo agents at the airport. Specific security requirements for PNG ASL should be included in their security program required by Part 109. That document may be referenced here to avoid duplication but it is imperative that agency consult in the development of their programs to ensure there is no conflicting security procedures and measures. Agencies should also make copies of their security programs available to each other).*

#### **1.2.9. Border Control Authorities**

*(This Section should highlight the role and responsibility of the various border control agencies at the airport, including, Customs, Immigration and Quarantine. While each of these agencies have unique and focused areas of interest it is imperative to ensure that they recognize the important part they play in the achievement of broader security outcomes. Specific mechanisms for sharing information that becomes known during the course of their normal duties, should be noted here).*

**1.2.10. Ground Handling Service Providers**

*(This Section should highlight who is responsible for the delivery of ground handling activities at the airport. This may be airline employees or a local third party. Specific reference should be made to their compliance with both the airline and airport security programs).*

**1.2.11. General Aviation Operators**

*(This Section should highlight that general aviation operators are an essential part of the airport security network and must remain vigilant in the identification of security breaches and vulnerabilities. It is imperative that access to secure areas be of an equivalent standard through airport tenancies as it is through dedicated access control points, including GA hangars).*

**1.2.12. Airport Tenants**

*(This Section should address the specific requirements for any leased areas at the airport, whether directly or indirectly involved in civil aviation operations. It is imperative that access to secure areas be of an equivalent standard through airport tenancies as it is through dedicated access control points, including GA hangars).*

**1.3. COORDINATION AND COMMUNICATION****1.3.1. Airport Security Committee**

*(This Section should outline the role of the Airport Security Committee. Specific details such as the terms of reference, membership and frequency of meetings can be included as an appendix. It should also address how minutes of the meeting are dealt with in terms of distribution and action items).*

**1.3.2. Communication with Stakeholders**

*(This Section should recognize that the key mechanism for communication at the airport is the Airport Security Committee, however additional means of communication, such as newsletter or airport community town hall meetings, may be required due to restriction on membership of the higher level committee. A full contact list of all stakeholders and tenants should be included as an appendix).*

**1.3.3. Management of Classified Information**

*(This Section should denote how any classified or security sensitive information that is received at the airport is managed, disseminated and stored).*

**1.3.4. Management of Media Requests**

*(This Section should clearly state how requests for information from the media should be managed. It may be that the only details provided to the media come from the most senior person at the airport or the senior executive of the airport operator).*

## **2. DESCRIPTION OF AIRPORT**

### **2.1. PHYSICAL CHARACTERISTICS**

#### **2.1.1. Airport Location**

*(This Section should include a broad description of the location of the airport in terms of the province and possibly geographical co-ordinates).*

#### **2.1.2. Airport Plans**

*(This Section should include maps and diagrams that depict the geographical location as well as clearly defined landside and airside areas. There should also be plans of terminal buildings depicting access control points, screening points and sterile areas. These should be included as an appendix).*

#### **2.1.3. Airport Facilities**

*(This Section should outline what facilities exist at the airport, include air traffic, weather and fuel, as well as terminal(s) and hangars).*

#### **2.1.4. Airport Operations**

*(This Section should outline the nature of civil aviation operations occurring at the airport and may include, international, domestic and general aviation operations. It should also include details of operational times and whether it has overnight operations and/or overnighing aircraft which require specific additional security measures).*

## **3. AIRPORT SECURITY MEASURES**

### **3.1. OVERVIEW**

*(This Section should reference Section 1.2.3 and include additional detail relating to any third party security service providers that are contracted to deliver security measures and procedures. This should include security service providers conducting activities in landside areas as well as within the terminal and in security areas. It should also be mentioned here if different security service providers are engaged by airlines or airport tenants to ensure a complete picture).*

### **3.2. LANDSIDE SECURITY**

### **3.2.1. Management of Terminal Curbside and Carparks**

*(This Section should address how the airport manages its landside areas with a specific focus on carparks and the parking of vehicles at the terminal curbside).*

### **3.2.2. Management of Unattended Vehicles**

*(This Section should specifically detail unattended vehicles and how they are treated).*

### **3.2.3. Management of Terminal Public Areas**

*(This Section should address how the airport manages its landside areas with a specific focus on public areas of terminal buildings, such as check in and arrival areas).*

### **3.2.4. Management of Unattended Baggage or Items**

*(This Section should specifically detail unattended baggage or items and how they are treated).*

## **3.3. AIRSIDE SECURITY**

### **3.3.1. Designation of Security Areas and Enhanced Security Areas**

*(This Section should reference the establishment of Security Areas in accordance with the Civil Aviation Act. It should also make mention of how Security Areas may be identified by signage. A description of what Security Areas are established at the airport could be provided here and should be supported by the diagrams and plans referred to in Section 2.1.2. A sample of the Security Area signage should be included as an appendix).*

### **3.3.2. Airport Permit System**

*(This Section should detail the implementation of the airport security identification card system. It should highlight the background checking requirements and any additional information relating to training or induction before the issue of a card, including airside driving requirements. This would include both individual and vehicle permits).*

### **3.3.3. Perimeter Security**

*(This Section should denote the physical security measures for the perimeter of the airport, noting the specific requirements contained within Rule Part 139. It should include a description of the fence and the location of any gates or other access points, including hangars and tenancies that have access to airside).*

### **3.3.4. Access Control**

*(This Section should detail the access control measures used to restrict unauthorized or unintended access to operational or security areas at the airport. This should include procedures for checking of permits and vehicle airside authorities).*

### **3.3.5. Screening of Airport Workers**

*(This Section should detail the requirements for screening of airport workers having access to secure areas, including sterile areas).*

### **3.3.6. Inspection of Airside Vehicles**

*(This Section should detail the extent of any vehicle inspection or search that is conducted prior to allowing a vehicle to access a secure area at the airport).*

### **3.3.7. Escort Procedures**

*(This Section should describe the escort provisions that are in place for allowing people who don't hold an airport security identification card or a vehicle airside permit however require access to a secure area for a legitimate purpose, such as maintenance workers).*

### **3.3.8. Mobile Patrols**

*(This Section should detail what procedures are in place to ensure that regular mobile patrols are conducted to ensure the integrity of the airport perimeter is maintained. The requirements contained in Part 139 should be complied with).*

### **3.3.9. Key Control System**

*(This Section should detail what system is in place for securing access control points both in the perimeter of the airport and within the terminal and/or hangars. This may be a key lock system or a secure code system. Details should include what measures are taken if a key is lost or stolen or a breach of security is identified).*

### **3.3.10. Protection of Aircraft**

*(This Section should denote what measures are employed to protect aircraft while on the ground at the airport. This may include static guarding or the use of mobile or foot patrols. Special consideration must be given to overnighing aircraft).*

### **3.3.11. Protection of Baggage Being Moved Around the Airport**

*(This Section should discuss what measures are used to ensure that baggage, after it has been accepted and screened, is protected from interference while in the baggage make-up area and when being moved around the airport for loading on an aircraft).*

### **3.3.12. Protection of Cargo and Mail Being Moved Around the Airport**

*(This Section should discuss what measures are used to ensure that cargo and mail, after it has been accepted and screened, is protected from interference while in the cargo shed and when being moved around the airport for loading on an aircraft).*

### **3.3.13. Protection of Navigational Aids and Vital Facilities**

*(This Section should highlight any specific security responsibilities that the airport has for vital facilities, including air navigation aids that are within the airport perimeter. It is appropriate to cross reference the need for other stakeholders to have primary responsibility, where appropriate).*

## **3.4. SCREENING REQUIREMENTS**

*(It should be noted that references can be made in the following Sections to the specific requirements contained in the Rule Part 140 exposition, without the need to duplicate the full details here).*

### **3.4.1. Sterile Areas**

*(This Section should discuss and describe the establishment of a sterile area for holding passengers that have been screened and cleared prior to boarding their flight. This area should be included in the diagrams and plans referenced in Section 2.1.2).*

### **3.4.2. Screening Equipment**

*(This Section should outline what screening equipment is available for screening of passengers and their baggage).*

### **3.4.3. Prohibited Items**

*(This Section should recognize acceptance of the Prohibited Items List included in the Part 139 Advisory Circular as being the standard to which screening is conducted).*

### **3.4.4. Separation of Screened and Unscreened Persons**

*(This Section should highlight what measures are in place to ensure that screened passengers do not mingle with unscreened passengers and airport workers after screening and before boarding the aircraft).*

### **3.4.5. Sterile Area Breach**

*(This Section should highlight what procedures are followed when a breach of the sterile area has been identified).*

### **3.4.6. Screening of Passengers and Crew**

*(This Section should discuss the requirement for screening and make mention of any exemption that may be in place, however the specifics of how screening is conducted can be dealt with by reference to the Rule Part 140 exposition).*

### **3.4.7. Screening of Cabin Baggage**

*(This Section should discuss the requirement for screening and make mention of any exemption that may be in place, however the specifics of how screening is conducted can be dealt with by reference to the Rule Part 140 exposition).*

### **3.4.8. Screening of Checked Baggage**

*(This Section should discuss the requirement for screening and make mention of any exemption that may be in place, however the specifics of how screening is conducted can be dealt with by reference to the Rule Part 140 exposition).*

### **3.4.9. Passenger and Checked Baggage Reconciliation**

*(This Section should discuss the process for ensuring only baggage that has been accepted from a passenger who is boarding the flight and the baggage has been subsequently screened is reconciled before the flight departs. This may include the use of bingo card or automated systems. It should be noted here that the baggage of any passenger who fails to board will be removed prior to departure).*

### **3.4.10. Screening of Goods Taken Into the Sterile Area**

*(This Section should detail the requirements for screening of goods taken into the sterile area for sale or to be provided to passengers in any available airline lounge).*

## **4. HEIGHTENED THREAT**

### **4.1.1. Additional Security Measures**

*(This Section should detail what additional measures may be put in place in the event of a heightened threat environment. This may eventuate due to a nationwide threat or a specific threat related to a local civil matter. Measures may include the employment of additional security guards, additional checks and searches of persons and vehicles accessing secure areas and/or additional lighting of airport and terminal areas at night).*

## **5. RESPONSE TO ACTS OF UNLAWFUL INTERFERENCE**

### **5.1. ACT OF UNLAWFUL INTERFERENCE**

*(This Section should cross reference requirements contained in the National Civil Aviation Security Program for management of an act of unlawful interference with civil aviation. It should also discuss the specific reporting requirements contained in Rule Part 12).*

#### **5.1.1. Emergency Operations Centre**

*(This Section should discuss whether an Emergency Operations Centre has been established and if so, where it is and who would be required to attend in the event of an emergency situation. It may even outline some of the event scenarios that would trigger the activation of the EOC).*

### **5.1.2. Bomb Threat**

*(This Section should detail the local method for dealing with a bomb threat. If bomb threat management information is made available to stakeholders, a copy of the document should be included as an appendix).*

### **5.1.3. Civil Unrest**

*(This Section should discuss the local method for dealing with incidences of civil unrest. This may include procedures for notifying airlines to prevent aircraft from landing for a period, if possible).*

### **5.1.4. Cyber Security**

*(This section should detail the implementation of measures to prevent and procedures to respond to a cyber-attack or corruption of information technology networks and systems).*

## **6. TRAINING**

### **6.1.1. Security Awareness**

*(This Section should detail how security awareness training is provided to the airport community and the frequency of recurrent training. It may include the use of newsletters or airport community town hall meetings).*

### **6.1.2. Airport Security Staff**

*(This Section should outline the specific training requirements for security staff who are airport employees. This will need to take into consideration the stated training requirements in Rule Part 140, depending on their role and responsibility).*

### **6.1.3. Contracted Service Providers**

*(This Section relates to Rule Part 140 certificate holders who employ third party contractors as security service providers to deliver certain elements of their Rule Part 140 certification, which may include screening. A cross reference should be made to the specific training requirements included in Rule Part 140).*

### **6.1.4. Screener Certification**

*(This Section should include a commitment to comply with the screener certification requirements outlined in the national level security programs).*

## **7. SAFETY AND QUALITY MANAGEMENT SYSTEMS**

*(This Section should reference the requirements under Rule Part 139 and Rule Part 100).*



**8. APPENDICES**

- A. Maps and Plans of the Airport
  - a. total geographical area owned and operated by the airport, including landside and airside
  - b. map of the airport perimeter showing access control points and airside security areas
  - c. diagrams of terminal buildings showing access control points and sterile areas
- B. Contact List
- C. Airport Security Committee Terms of Reference and Membership
- D. Sample Security Area Signage
- E. Sample Airport Security Identification Cards and Vehicle Permits