REPUBLIC OF ALBANIA

ALBANIAN CIVIL AVIATION AUTHORITY

GUIDANCE MATERIAL FOR THE SECURITY MEASURES ON AIRPORT PERIMETER PROTECTION

ACAA-DAS-GM5-SMAP

Issue: 01, Revision 00

Date: 27.03.2024

Approved by:

Maksim Et'hemaj

Executive Director of the Civil Aviation Authority

Intentionally left blank

0 ADMINISTRATION

Table of Contents

0.3 Review Table

Page #	No. Release	No. Review	Date	Reviewed by:

0.4 Distribution List

Control #	Responsible Persons	Document Type
Original	SCOS/SSS	On paper
Electronic	DAS staff	Electronic copy in DRMS

0.5 Definitions

For the purpose of this guidance manual, the following terms mean:

Airport *(Airport)* means the area which is open for commercial air transport operations in Albania.

Acts of unlawful interference *(Acts of unlawful interference)* are those acts or attempted acts that as such endanger the security in operation (security) of civil aviation, but not limited to:

- unlawful possession of the aircraft,
- destruction of an aircraft in service,
- hostage taking on board the aircraft or at the aerodromes,
- forcible entry on board an aircraft, at an airport or aeronautical building facilities,
- bringing on board an aircraft or at an airport a weapon or dangerous equipment or material for criminal purposes,
- using an aircraft in service with the intention of causing death, serious bodily injury or damage to property or the environment,
- the communication of false information which as such endangers the techno-operational security of the aircraft in flight or on the ground, passengers, crew, ground service personnel or the public in general, at an airport or in the facilities of an aviation building civil.

Behaviour Detection *(Behaviour Detection)***.** The application of techniques that include the analysis of behavioural characteristics, including but not limited to, psychological or gesticulation signs, indicative of abnormal behaviour, in order to identify persons who may pose a threat to civil aviation.

Vulnerability *(Vulnerability)* means any weakness in the implementation of measures and procedures which can be used to carry out an act of illegal interference.

Entity *(Entity)* means a person, organization or company, other than an operator.

Security control *(Security control)***.** A means by which to prevent the introduction of weapons, explosives or other dangerous devices and substances which may be used to commit an act of unlawful interference. substances and objects.

Access control (Access control) means the implementation of methods by which the entry of unauthorized persons or unauthorized vehicles or together can be prevented.

Security Culture *(Security Culture)***.** A set of security-related norms, values, behaviours and assumptions present in the day-to-day operation of an organization and reflected in the behaviours and actions of all entities and personnel within the organization.

Unpredictability(*unpredictability).* Implementation of security measures in order to increase their preventive effect and efficiency, applying them at irregular frequencies, in different places and/or with different means, in accordance with a defined work framework.

Critical parts of security restricted areas *(Critical parts of security restricted areas)* means at least those parts of an airport where more than 60 persons hold airport identification cards which give them access to restricted security areas to which passengers scanned at departure have access and those parts through which they can pass through or they may be held in the hold's scanned baggage, except when related to checked baggage.

Aviation security *(Aviation security)* means the combination of measures and material and human resources in order to protect civil aviation from acts of illegal interference that endanger the security of civil aviation.

Terminal *(terminal)* means the main building or group of buildings where the processing of passengers for commercial and delivery purposes and check-in for aircraft takes place.

Security Restricted area *(Security restricted area)* Those parts of the airside which are identified as priority risk areas, where in addition to entry control, other security controls are applicable.

Demarcated area *(Demarcated area) means* an area that is separated by means of entry control either from security restricted areas or if the segregated area is itself a security restricted area from other security restricted areas at an airport.

Landside *(Landside)* means those parts of the airport, the surrounding territory and buildings or parts of which are not airside.

0.6 Abbreviations

The following abbreviations will be used in this guidance material:

ACAA	Albanian Civil Aviation Authority
DAS	Directorate of Aviation Security
DE	Executive Director
EDS	Explosive Detection System
OJT	On Job Training
NCASP	National Civil Aviation Security Programme
NCASTP	National Civil Aviation Security Training Programme
SRA	Security Restricted Area
UM	Minister Order
EC	European Commission
ICAO	International Civil Aviation Organisation
VKM	Council Of Ministers Decision
PIDS	Perimeter Intrusion Detection System

1. SCOPE & APPLICABILITY

1.1 The purpose

The purpose of this procedure is to provide guidance in regard to perimeter protection to deter inadvertent or premeditated access by an unauthorized person to the airside area and also general regulation and guidance governing the operation of security patrols at an airport. Applicable measures from each entity and responsibility are included in this document.

1.2 Legal Basis

This guidance material is based on the following legal references

- DCM No 1115, dated 24/12/2020, "On Approval of National Civil Aviation Security Programme"
- DCM No 821, date 24.12.2021, "Designation of basic standards for safeguarding f civil aviation from unlawful Interference act that threatening civil aviation security."
- Minister Order No 163 date 26/03/2021, "On Detailed Measures for Implementing common fundamental standard in the security of civil aviation"
- Minister Order No 26, date 20.10.2010 on "General regulations in the civil aviation security".
- ICAO Aviation Security Manual (Doc 8973) latest edition

2. SCOPE AND OBJECTIVES

The objectives of this Guidance Manual are to provide:

a) A generic guidance for airports and other entities that are implementing physical security measures on the best practices for airport perimeter protection measures, including perimeter fence, lighting, use of CCTV etc.;
b) Guidance material for security patrols and how to effectively use this mean of surveillance to prevent, deter and detect any suspicious behaviour or attempted act of unlawful interference.

2.1 Airport Perimeter security

Protection of security restricted areas is one of the main requirements of aviation security, whereas perimeter security and surveillance measures are some of the means used for this purpose.
This section describes physical protection for the airside and landside perimeter, including specifications for:

a) the perimeter fence or other perimeter security provisions;
b) lighting;
c) warning signage;
d) intrusion detection;
e) closed-circuit television (CCTV) surveillance; and
f) patrols (frequency and records keeping).

Particular consideration should be given to areas of the airside and landside interface that cannot be protected in the usual ways, such as baggage belts from the check-in area leading into the baggage hall. A general description should be included of how unauthorized access via these routes is prevented. This section should also describe the number, location and hours of operation of designated pedestrian and vehicular access points, as well as the location of airport emergency gates.

2.1.1 Airport perimeter protection

The purposes of a fence are to demarcate the perimeter, deter unauthorized access, delay intrusion and aid in the detection of intrusion. These purposes should be considered during the design of an airport fence and should be commensurate with the assessed risk from unauthorized intrusion.

The level of protection offered by a fence will depend on its height, method of construction, the material used and any additional security features used to increase its performance or effectiveness, such as barbed wire topping, a perimeter intrusion detection system (PIDS), lighting or a closed-circuit television (CCTV) system.

More information on the use of CCTV systems as a security tool can be found in Appendix 1.

Fences between the landside and airside should be physical obstructions that are clearly visible to the general public and deny unauthorized 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.

Due to safety and operational reasons, at certain locations on the perimeter, particularly the take-off and landing runway thresholds, metal fences cannot be used, since they might disrupt the operation of navigation aids. 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.

2.1.2 Clear zones and signage along the perimeter fence/barrier

The entire fence area should, if possible, be visible to resident or patrolling guards. It may prove necessary to shorten the perimeter in places to avoid pockets in the fenced area which could otherwise be out of sight. This not only applies to walls and opaque fences but also to transparent fences, since these commonly become opaque when viewed from an oblique angle. Alternatively, a CCTV system may be used. Transparent fences are usually preferable to opaque fences as they allow guards to see outside the protected area.

In selecting the most appropriate fencing material, consideration should be given to the other components of a perimeter security system. For example, if a fence is used with a PIDS, and is supported by appropriate perimeter lighting, a CCTV system, warning signs and frequent patrols, it may be possible to use a more general type of security fence. In areas where such systems are not available, a higher grade

security fence should be used to increase the length of time it may take an intruder to cut through or climb the fence as well as augmenting the level of difficulty of doing so.

2.1.3 Maintenance of fence/barrier

Consideration should be given to the ongoing maintenance of the fence and the ease of replacement of sections that become damaged or unserviceable such as through corrosion. The use of galvanized or plastic-coated fencing may be most appropriate in locations where corrosion is likely to be a problem.

The type of fence chosen should reflect the type of threat expected and be compatible with the terrain and with any requirement for intrusion detection and/or CCTV systems. The fence should, whenever possible, be run in straight lines for ease of erection and surveillance. Junctions where a fence changes direction are usually easier to climb and should therefore be kept to a minimum. As much as possible, junctions that turn outwards should be avoided as these are the easiest to scale.

Whenever possible, the ground on both sides of a perimeter fence should be cleared in order to establish an exclusion zone (a distance of about 3 m from the fence is recommended) that would remove cover for any intruders, and should be kept clear of obstructions, such as lamp posts, signposts, equipment, vehicles, and trees, that may assist an intruder to climb the fence. The fence may have to be set back from the actual site boundary to leave an unobstructed area outside the fence.

2.1.4. Patrol road alongside the fence

A patrol road suitable for vehicles should be constructed alongside the fence to permit the passage of motorized patrols, ideally on both the landside and airside, but if not both then definitely the airside. The road should be well drained and kept free of obstacles at all times.

Vulnerable points and/or key airport installations, such as the fuel farm and air navigation facilities, located on the airside within the aerodrome enclosure should be surrounded by an appropriate perimeter fence constructed to at least the same technical specifications as the aerodrome land perimeter described above.

The effectiveness of any security perimeter will depend to a large extent on the level of security at the points of entry. Gates should be constructed to the same security standard as perimeter fences, and some form of access control should be in place. Without such control, the security of the entire fence will be negated. An added value and also very effective measure is Perimeter intrusion detection combined with CCTV systems

Generally, fencing systems are not able to detect intrusion and a PIDS should therefore form part of an overall perimeter security system. A PIDS is an electronic device designed to discern the entry or attempted entry of an intruder across the external perimeter or protected area, identify the location and generate an alarm. When properly deployed, such a system can enhance the effectiveness of other perimeter defences, but is prone to false alarms and should therefore be used with an alarm verification system such as CCTV. A PIDS may be installed as a covert device, or overtly to act as a deterrent.

The use of a CCTV system for surveillance may save on human resources while covering large sites or perimeters, especially when used in conjunction with intrusion detection and automated access control systems, and may supplement or extend an existing security system. Such a system also enhances the effectiveness of perimeter security, particularly when used to verify alarms activated by a PIDS. A CCTV system may also improve working conditions for security guards by allowing them to avoid exposure to danger as well as inclement weather and other inconveniences of routine patrolling. A system's effectiveness will depend, however, on the selection of suitable equipment and the method of installation. *More information on a PIDS and on CCTV systems is provided in Appendix 1.*

2.1.5. Emergency gates

Emergency gates, also known as crash gates, are often installed in an airport's perimeter fence to allow the quick access or egress of emergency service vehicles to on-airport or off-airport aircraft accidents. Crash gates should be constructed to maintain the integrity and standard of the perimeter fence and should be locked or guarded, and preferably kept under continuous surveillance. The fitting of frangible links in locking systems is a useful means of allowing emergency vehicles access or egress while not compromising security. Consideration should also be given to equipping such gates with intrusion detection systems.

2.1.6. Security lighting

Security lighting can offer a high degree of deterrence for potential intruders, in addition to providing the illumination necessary for effective surveillance, either by guards, motorized patrols or indirectly through a CCTV system. There are various types of security lighting to meet particular applications:

a) Perimeter lighting is designed to cast a strong light on the perimeter, with overhead lamps or low mounted lamps that create a glare effect to dazzle and deter intruders. If the latter are used, care should be taken to ensure that they do not create a nuisance or hazard to aircraft;

b) Area lighting is intended to illuminate areas inside the perimeter through which intruders may cross in order to reach their objectives. This increases the guards' ability to detect intruders and acts as a powerful deterrent. Ideally, the illumination should be even and without shadows. Every part of each area to be illuminated should be lit by at least two lights to guard against lamp failure;

c) Local lighting is used to illuminate those areas inadequately covered by area lighting and which might conceal an intruder. Small bulkhead lights, tough and resistant to interference, should be used. Fluorescent or tungsten-halogen lamps may be used as miniature floodlights. All dark spots should be eliminated. Roofs, fire escapes and emergency exits should be illuminated by such local lighting; and

d) Floodlighting is designed to illuminate surfaces such as buildings and fences that intruders may pass in front of to reach their objectives. At the low illumination levels typical of a security lighting situation, the eyes rely mainly on the ability to recognize outline shapes. A moving silhouette can readily be seen against an illuminated wall, preferably painted white or some other light colour.

Security lighting acts as a particularly good low-cost deterrent as a low level of illumination will deter most potential intruders and vandals. If a CCTV system is installed, the lighting level and uniformity should be such that they help to present a clear monitor picture to security guards.

The frequent inspection and maintenance of security lamps are necessary as light output decreases significantly after prolonged use. Lamps requiring long warm-up periods are unsuitable for certain security lighting applications. Time switches, movement sensors or photo-electric sensors may be useful for the control of security lighting, but the latter are vulnerable to deliberate interference.

3. AIRSIDE AND SECURITY RESTRICTED AREAS

The airside is that part of an airport where aircraft and supporting vehicles normally move about, together with the adjacent terrain and buildings or portions thereof, access to which is controlled.

Security restricted areas should be established at each airport serving civil aviation designated by the State, according to the results of security risk assessments carried out by the relevant national authorities.

More information on security risk assessments can be found in Appendix 2.

Security restricted areas are located airside of an airport, and are identified as priority risk areas where, in addition to access control, other security controls should be applied. Such areas will normally include, inter alia, all commercial aviation passenger departure areas between the screening checkpoint and the aircraft, the ramp, baggage make-up areas, including those where aircraft are being brought into service and screened baggage and cargo are present, cargo sheds, mail centres, airside catering and aircraft cleaning premises.

In keeping with the key security principle of defence in-depth, whereby limited security resources are allocated for the protection of the most likely target, with layers of defence radiating outward, States should limit the size of their security restricted areas to an expanse that can be effectively secured and which ensures that resources are not too widespread.

Security restricted areas should therefore be kept as small as possible, in proportion to the level of aircraft operations and the quantity of security resources. Resources should be allocated to the most likely targets in a manner that is effective and in line with the current threat assessment level. This approach allows, for example, the implementation of higher access control standards for those persons and vehicles that are required to approach and service an aircraft, than for all vehicles moving around the airside, as shown in Figure 1.

Access points from public areas to security restricted areas should be kept to a minimum and should have effective access control measures or be kept locked. Access by staff to security restricted areas should be limited to those with a clear operational need to enter by virtue of their duties. Similar controls should apply to vehicles, with access granted to only those vehicles clearly required for operations.

Security restricted areas not subject to continual access control measures should be thoroughly searched prior to being used. Figure 1.

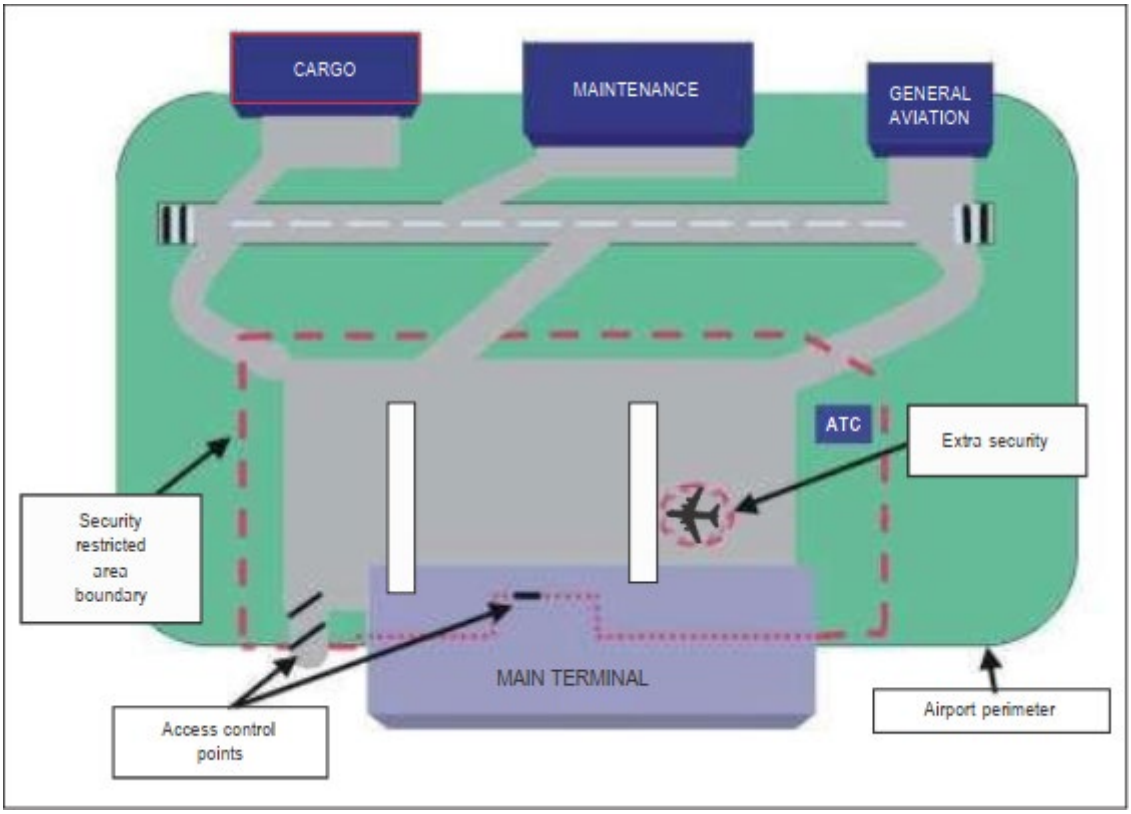

Figure 1

3.1 Access control points and suggested boundary of a security restricted area

Regulations defining the location and function of security restricted areas are published by CAA and made known to all organizations and persons requiring access to the airside or a designated security restricted area.

The enactment of appropriate legislation or regulations that impose penalties on any person wilfully trespassing or attempting to trespass into the airside or a designated security restricted area is essential. Such legislation or regulations should also include penalties for wilful or attempted trespassing at off-airport communications and air navigation aid sites.

Unauthorized persons found within a designated security restricted area or other operating area at the airport or related aeronautical facility should be detained and, if warranted and permitted, searched and interviewed to ascertain if there are suspicious or criminal intentions. Reports of such incidents should be filed with the airport security officer and relevant policing authorities.

3.2 Physical security measures

Both airside and security restricted area perimeters should 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 should 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, should 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 should 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 should 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 should 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 should be supported by properly trained personnel, sound and comprehensive contingency planning, and concise, well written security plans and orders

3.3 Access control points

3.3.1 Protection of Emergency Exit Doors

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 centre. 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.

3.3.2 Access Control for Hold Baggage Handling System

To prevent the introduction of unauthorized 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 authorized personnel should be allowed access to the baggage system.

3.3.3. Restrictions on entering a Security Restricted Area

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 should be secured when not in use.

3.3.4 Designation of External Access Control Points

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
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.

3.4 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.

3.5 Lock and key controls

A lock and key control system should be established at each airport. Such a system should identify the type of lock and key 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.

4. SURVELLIANCE, PATROLLING AND OTHER PHYSICAL SEARCHES

In the Airport and elsewhere is possible, the area near to the landside, perimeter fence, and other sensitive areas shall have surveillance, patrolling and other physical search in order to identify persons with suspicion behaviour, vulnerabilities than can be used to commit an act of unlawful interference and to prevent the persons to undertake such act.

4.1 Objectives of Security Patrols

Observation or patrols should be undertaken with the aim of monitoring:

(a) Divisions between the public area, the air zone, security restricted areas, critical parts and, where possible, separate areas; and
(b) Areas of, and in the vicinity of the terminal, that are possible for public access, including parking areas and roads; and
(c) The display and validity of persons' identification cards in restricted security areas other than those where passengers are present; and
(d) The display and validity of vehicle licenses when in the air zone; and
(e) Baggage of the barn, cargo and mail, in-flight supplies and mail and air carrier and materials in critical parts waiting to be loaded.

4.2 Frequency and Means, Modes of Observation

Frequency and means, the modes of undertaking surveillance and patrols must be based on a risk assessment and approved by the Civil Aviation Authority. They should take into account:

(a) The size of the airport, including the number and nature of the operations; and
(b) The design of the airport, in particular the interaction between the areas located at that airport; and
(c) Possibilities and limitations of vehicles for the surveillance and patrol undertaking.

Parts of the risk assessment related to frequency and means, the means undertaken for surveillance and patrols shall, upon request, be made available in writing for the purposes of monitoring compliance.

4.3 Unpredictability

Patrolling should be implemented in a random and unpredictable way (e.g. spot checks), so that patrols cannot be avoided or bypassed as a result of hostile reconnaissance or insider knowledge. Additionally, patrolling should not only focus on the surveillance of airport personnel but include passengers, other airport stakeholders, and airport infrastructure and goods for signs of unusual activity or poor security. Patrolling can be effective as a visual deterrent if personnel are in uniform and use marked vehicles. Alternatively, patrolling can provide increased surveillance if conducted covertly.

4.4 Tools, Modes of Observation

The following tools may be used as a mean of observation and surveillance:

a) CCTV
b) Patrolling of the airport perimeter (Mobile Patrol).
c) Patrolling of the Main Terminal Building (Foot Patrol).
d) Patrolling the apron area (Foot patrol).

Appendix 1

INTRUSION DETECTION AND CCTV SYSTEMS

1. INTRUSION DETECTION SYSTEMS

General

1.1 An intrusion detection system is designed to detect the entry or attempted entry of an intruder into a protected area, to identify the location of the intrusion, and to signal an alarm to a response force.

1.2 An intrusion detection system is classified according to the level of security it offers. A Class 1 system offers the lowest level of security and a Class 4 system the highest, as follows:

a) class 1 – an alarm system for use in low-risk premises where potential intruders have little Knowledge of alarm systems and a limited range of readily available tools. Such systems are unlikely to have an appointed response force but will rely on a public response to a local alarm or strobe lights;

b) class 2 – an alarm system normally used in premises where the risk of a sophisticated attack is not high. Intruders are expected to have a limited knowledge of alarm systems and have only basic tools and portable instruments available;

c) class 3 – an alarm system used in premises where high-value assets are held. Such a system will also include appropriate physical security protection. It should offer protection from intruders who are conversant with an intrusion detection system and have available a comprehensive range of tools and portable electronic equipment; and

d) class 4 – an alarm system intended for use in applications where security takes precedence over all other factors. It is intended to offer a level of protection from intruders who are expected to plan an intrusion in detail and have a full range of equipment capable of disabling vital system components. A Class 4 system will need to be supplemented with comprehensive physical security measures and procedures.

1.3 An intrusion detection system provides continuous coverage of the protected area and, when used in conjunction with a CCTV system, may extend coverage into areas not normally accessible to guard patrols, such as a roof space or locked rooms. An intrusion detection system should be viewed as a component of the perimeter security system, rather than as a stand-alone system.

Installation

1.4 Care should be taken in the selection, application and installation of an intrusion detection system in order to ensure that there are no blind spots and to minimize environmental interference and spurious alarms. In preparing a request for a proposal, the end-user requirements for an intrusion detection system installation should specify:

a) the area and/or equipment to be protected;

b) the level or degree of threat;

c) whether linkage to other electronic systems is required, such as CCTV or automated access

control;
d) whether the protected area will have an on-site guard force or a signal to a response force; and
e) the type of reaction force or monitoring arrangements required.

System components

1.5 An intrusion detection system installation will normally include some or all of the following system components:

a) detection sensors;
b) control panel with optional event recorder and printer;
c) alarm display;
d) alarm signalling link between control panel and alarm display;
e) installation wiring;
f) reaction force; and
g) independent or back-up power supply, as appropriate.

Detection sensors

1.6 Detection sensors are designed to detect an intrusion within the area they cover and to provide an indication to the control panel of the alarm condition. Different types of sensors are available, the choice of which will depend on the nature of the location to be protected, and different types may be used in combination to cover technical vulnerabilities, reduce the incidence of false alarms, and provide against failure. The most appropriate installation will concentrate intrusion detection system sensors on points of entry such as doors and windows.

Types of sensors

1.7 Various types of detection sensors are available and are divided into the following categories:

a) contact sensors, which cover various switching devices such as micro-switches, magnetic reed switches, pressure pads and some types of vibration sensors. Switches can be used in either make or break mode, that is, open or closed circuit, but care should be taken to ensure that an accidental or deliberate loss of power will cause the system to fail safe and raise an alarm. In high-security installations, magnetic reed switches should be of the double-reed type, which incorporate a tamper protection switch;
b) spatial or volumetric sensors, which are designed to detect movement within their field of view and are used to cover rooms, corridors, roof spaces and other open areas or entry routes. Ultrasonic sensors use high-frequency sound waves and the Doppler effect of radiated and reflected transmissions. They are reliable and difficult to defeat but can generate false alarms from air turbulence or extraneous sounds such as telephone bells. Passive infrared sensors monitor the infrared heat profile of an area and detect changes caused by human intrusion. Microwave sensors use high-frequency radio transmissions and reflection to detect movement. Because of the

penetrating properties of microwaves, careful installation is necessary to avoid false alarms caused by movement outside the protected area;

c) beam interruption devices, which are usually of the active infrared type, and use a transmitter and receiver and sometimes reflecting devices to project a beam across an opening such as a door or window. When the beam is broken, either by the opening of the door or window or by a person passing through it, an alarm is raised.

d) vibration detection devices, which detect vibrations by various devices or technologies, such as: an inertia switch that reacts to vibration or impact with a contact ball that bounces or lifts off its contacts and produces an alarm condition; a geophone that detects movement with a suspended magnet moving inside a detector coil; or piezoelectric crystals that produce an electric current from structural pressures. Once vibrations are detected, an alarm is raised; and

e) dual technology sensors, which are devices that combine two sensor technologies such as passive infrared and microwave in one housing, where they work together before signalling an alarm. In this way, the likelihood of false alarms is greatly reduced. Dual technology sensors should be used with care and only where the local conditions allow no alternative, since the danger exists that the overall sensitivity of the system may be reduced if there is a requirement for two devices to be activated together before an alarm is sent.

Control panel

1.8 The main functions of a control panel are to:

a) monitor the state of detection sensors;
b) detect tampering;
c) allow the system to be turned on and off; and
d) signal an alarm state.

Event recorder

1.9 More sophisticated control panels built around microprocessors usually include an event recorder or electronic log that can be linked to a hard copy printer. The recorder provides a log of all alarms and operational instructions, such as the setting and unsettling of the system. Such a recorder should provide a useful aid for monitoring the security of the system, as well as an audit trail. Unless the control panel is situated at a permanently staffed guard point, it should be located at the heart of an intrusion detection system installation, where it is given maximum protection both by the system itself and by other physical security measures.

Alarm display

1.10 An alarm should be signalled to a permanently staffed control position from where the appropriate response can be made. Alarms should normally be given by both audible and visible means and should identify the location and type of alarm. In sophisticated systems, computer graphics and visual display units may be used to indicate the particular zone or areas in which the

alarm has occurred and the actions to be taken by the guard.

1.11 In low-risk sites covered by commercial and/or domestic burglar alarm equipment, the alarm signalling may be provided by an external alarm bell and strobe light. Such systems usually rely on a public response to the alarm as there is not normally a designated response force. The use of publicly audible and/or visible alarm signals in high security installations is not generally recommended, as such alarms indicate to an attacker where alarm sensors are installed and what reaction an alarm will cause, and the vulnerabilities of the system can then be identified and exploited.

Alarm signalling

1.12 Some form of remote alarm signalling to an alarm monitoring station will be necessary if the protected site is remote or not permanently staffed. Alarm signals may be communicated via different means. The most common are described below:

a) private wires – direct telephone lines used exclusively for alarm signalling and monitoring. This system provides protection against shorting out or cutting the lines, which will cause an immediate alarm. Private wires can be expensive;
b) auto-dialling – a standard exchange telephone line and equipment that, when an alarm is raised, automatically dials an emergency call number and relays a pre-recorded message. For this system the line should be ex-directory or selected as an outgoing calls only system. This will guard against the line being blocked by incoming calls, which would prevent the transmission of an alarm. These systems do not allow for permanent line monitoring and cannot immediately identify line faults or cut lines. They are therefore not recommended for high-security installations; and
c) radio-links – provide a multipath communications system which can incorporate a number of features such as automatic paging, data encryption and two-way interrogation and response protocol. The selected system and the facilities offered will need to be carefully considered to ensure the appropriate level of security is achieved

Installation wiring

1.13 The installation wiring in a high-security system should be monitored automatically at all times. In other words, there should be continuous electronic examination of the circuit connections to ensure that they are in working order and are not being tampered with. There should be an immediate alarm if a fault occurs or line tampering is detected. The level of line monitoring in installations of a lower security standard is normally only suitable for use within the protected area. Installation wiring that lies outside the protected area cannot be considered secure unless additional physical protection is provided, such as the use of protected ducts or armoured cables.

Reaction force

1.14 The intrusion alarms should be expeditiously responded to and validated. The response time should be as short as practicable and in any event should aim to identify, locate and intercept an intruder before

he or she can reach his or her intended target, such as the passenger apron, or carry out an attack.

Setting and un-setting

1.15 For unstaffed sites it is necessary to have a setting up procedure to allow the intrusion detection system to be switched on and off by authorized personnel without causing an alarm. Types of setting up procedures include the following:

a) automatic time setting, which allows the system to set and unset at a pre-set time;
b) a time delay, where the system allows a pre-set time elapse to permit the user to leave or enter the protected site after the set or before the unset procedure has been completed without raising the alarm. Time delay may not be appropriate in areas close to vulnerable points where a very quick intervention is required;
c) last exit system, in which the closure of the last exit door from a building or site activates the intrusion detection system through a switch mounted in the door frame or in the lock; and
d) a personal identification number key pad, which is placed outside the protected area and requires the entry of a code to set the system or to start the timed entry counter.

System management

Installation and maintenance

1.16 The integrity of an intrusion detection system depends on proper installation and maintenance. Circuit diagrams, manuals and spare components for intrusion detection system installations should always be kept under secure conditions. Likewise, all installation and maintenance work should be carried out by authorized personnel and supervised by security staff. Any modifications to the system should be recorded, and this record should be held with the original specification or diagrams.

A reserve power supply should always be available to enable an intrusion detection system to continue operating in the event that the main power supply fails or is disconnected. Float charge batteries are normally used for this purpose, and should have a sufficient capacity to cope with foreseeable contingencies. The condition of the batteries should be regularly checked by authorized personnel.

Access control panel

1.18 An intrusion detection system should only be set or unset by authorized personnel. The control panel should therefore be positioned and protected so as to deny access to all but nominated staff. If a control panel is key operated, the key should never be left in the panel and should be treated as a security key. Operating codes should be protected in the same way as combination lock settings or system passwords. If the control panel is sited within an area that is not permanently supervised, it may be necessary to prevent unauthorized access by securing it in an approved security cabinet or container. The container should be kept locked and protected by the intrusion detection system.

Access to sensors

1.19 Every effort should be made to ensure that unauthorized personnel do not have access to installed intrusion detection system sensors. The tamper alarms should be monitored continuously, and the correct operation of all sensors should be checked at regular intervals.

Walk-test lights

1.20 Walk-test lights, usually a red light emitting diode mounted on the front face of a sensor, indicate that the device is operating. However, this indication can be deceptive and should not be taken as a test of the system. The only effective way of testing an intrusion detection system installation is to activate a sensor and check that an alarm has been raised. Walk-test lights can also be an aid to an attacker by indicating the coverage or range of a sensor. It is therefore strongly advised that walk-test lights be masked or disconnected in all high-security installations.

Testing

1.21. An intrusion detection system installed in a high-security site should be tested at least once per day. If this is not possible, the system should be tested regularly at intervals to be prescribed in local security regulations. Such testing should include a check on the functioning and sensitivity of each individual sensor and on the correct receipt of the alarm signal at the control panel. Any malfunctions should be reported immediately for rectification by relevant security management.

Event logs

1.22 If event recorders are fitted, they should be examined regularly by security management staff and compared, where appropriate, to reports submitted by the guard force. Staff should be trained to recognize the development of a suspicious sequence of events and have the authority to investigate incidents. If a hard-copy printout of events is obtained, it should be stored for a period of not less than three years to allow for retrospective analysis and investigation.

Alarms

1.23 At times, alarms are signalled for which the cause is not readily apparent, and the signals dismissed without further investigation as likely to have been caused by an environmental factor or a technical fault in the system.
Doing so, however, ignores the possibility that the system may have been subjected to a deliberate attack. In the event of an attack being mounted on an intrusion detection system, a sensor may give only one warning before it is circumvented. Therefore, each alarm should be thoroughly investigated by security staff, if necessary in conjunction with an intrusion detection system engineer, and every attempt made to establish the cause. The possibility should also be considered that a sequence of unexplained alarms occurring over a prolonged period of time may indicate that probing attacks are being carried out or that an attacker is attempting to undermine confidence in the system.

Refurbishment of buildings

1.24 If buildings or individual suites of offices are refurbished after an intrusion detection system has been installed, the rearrangement of partition walls and repositioning of protected equipment may reduce the level of protection originally provided by the system. A new survey should therefore be carried out and the system installation adapted to the new accommodation arrangements. While building renovations are in progress, care should be taken to prevent building workers from having unsupervised access to components of the system, and a thorough check of the system should be carried out once the work is completed. If major alterations are involved, it may be necessary to decommission the system altogether until the work is finished.

CCTV SYSTEMS

General

2.1 A properly selected and installed CCTV system is an integral part of the entire security system, providing a range of benefits, including the following:

a) reduced dependence for surveillance on guards, reducing staffing requirements;
b) remote monitoring of the perimeter and other protected areas;
c) surveillance coverage at night and during inclement weather;
d) recording of events for playback and evidential purposes;
e) verification of alarms;
f) verification of identity and authorization for access in conjunction with an access control system;
g) coordination of responses to alarms and other operations; and
h) improved overall security

CCTV systems range from simple indoor or outdoor systems to complex, multi-camera, low-light-level systems. In the simplest system, a camera is linked by a cable to its own monitor, which is normally located in a staffed control centre. More complex systems include cameras fitted with zoom lenses and pan and tilt facilities, referred to as mobile cameras, and the use of artificial lighting, either visible or infrared, to provide 24-hour surveillance. The possible applications include supplementing intrusion detection systems such as the verification and checking of alarms, and monitoring of:

a) specific areas, such as parking;
b) pin-pointed areas, such as surveillance of equipment or entry points which could not otherwise be covered;
c) remote ATS sites or premises;
d) perimeter alarms; and
e) equipment.

Specifying operational requirements

2.3 It is important to clearly define the performance requirements of a CCTV system, which should cover:

a) the areas to be monitored and the purpose for which monitoring of each area is required, such as for access control or alarm assessment;
b) the picture quality required in each area monitored. For instance, the ability to identify people and permits may be required for access control, while less detail may be acceptable for other purposes;
c) whether linkage to an intrusion detection system is required;
d) the proposed monitoring requirements; and
e) any other performance requirements, such as the ability to operate in low light or provide anti tampering measures.

Site survey

2.4 A site survey should be carried out by day and night, if night-time surveillance is required, and include the following considerations:

a) *Terrain*. Different types of terrain, such as asphalt, open grassland or red brick buildings, will give different results from the same type of camera;
a) *Climate and environment*. Camera performance can be adversely affected by heat, ice, high rainfall, condensation, dust, etc. Cameras may be blinded by snow, fog, heavy rain or smoke. Special features such as sun shades, wipers and heaters may be required; and
b) *Existing light sources*. Camera performance may be impaired by existing light sources or conditions such as street lights, security lights, the reflection of sun off water or windows and light during sunrise or sunset. Such sources should be screened or the camera sited in order to avoid them.

Video and/or digital recording

2.5 Time-lapse videotape recording enables pictures covering periods of up to 300 hours to be recorded on single reel. The ability to record and play back is a useful feature for recording and investigating alarms.
2.6 Other types of recording media may be used according to predetermined specifications based on reliability and technological needs.

Video motion detection systems

2.7 A video motion detection device monitors the signal for movement or changes in light intensity in the picture and initiates an alarm when this occurs. The systems range from a single camera processor and monitor system to groups of cameras whose video signals are constantly assessed by a central processor. It should be noted that there are limitations to such systems, particularly when outdoor

applications are being considered. Changing light conditions and weather can affect performance. Also, the systems may have problems differentiating between authorized movement and unauthorized movement in an area under surveillance. Such systems may prove more operationally effective when used indoors, in environments which are more controlled.

CCTV system commissioning and audit test methodology

2.8 All security CCTV systems should always be commissioned and subsequently audited on a regular basis using an appropriate methodology. A CCTV system test methodology should test, measure and record the following criteria:

a) coverage;
b) target visibility;
c) target image height; and
d) system response time

2.9 The performance requirements for each criterion should be established in the contract specifications, and care should be taken to ensure that the methodology evaluates the criteria in a way that closely matches the operational requirements of the system.

Definitions and minimum standards
Coverage

2.10 The evaluation should confirm that the designated area is covered with the minimum of overlap. The degree of overlap is defined as the percentage of picture width for horizontally adjacent areas, or picture height for vertically adjacent areas. The minimum recommended overlaps are 5 per cent and 10 per cent, respectively

Target visibility

2.11 Target visibility is a measure of how easily a target can be seen on the monitor under worst-case illumination conditions. Using an appropriately camouflaged target, placed in the worst-case level of illumination and location, the operator should indicate whether the target is:

a) easily seen, that is the target is immediately obvious and no mistake is possible;
b) fairly easily seen, that is the target needs to be searched for but would not be missed and is found within the allowed system response time;
c) difficult to see, that is the target is only found after a careful and lengthy search exceeding the allowed system response time; or
d) not seen at all.

2.12 Only conditions specified under a) and b) should be acceptable as results.

2.13 The following examples can be used as camouflaged targets:
a) mannequin dressed in a camouflage jacket;
b) briefcase made dirty or muddy; or
c) number plates made muddy.

Target height image

2.14 Target image height is the height of the target image on the monitor screen as a percentage of the vertical picture height. The minimum acceptable image heights as a percentage of monitor screen height are
a) detection 10 per cent;
b) recognition 50 per cent; and
c) identification 100 per cent.

System response time

2.15 To measure system response time, the camouflaged target should be placed somewhere in the field of view and an alarm initiated. If a CCTV system is used in conjunction with a perimeter detection system, the response time is measured from the initiation of an alarm signal to the time when the operator has ascertained which monitor to view and has identified the target visually.

2.16 If a CCTV system is used separately, then system response time can be defined based on fixed operator search patterns and the cycle period of the search. The role of the operator is to react to an alarm activation and initiate response action within the stated response time.