AIRPORTS COMPANY
SOUTH AFRICA

Request for Proposal for the Supply, Installation and Maintenance of an Intelligent Integrated Security Platform

Annexure A – Scope of Work

Glossary and Abbreviations

Item	Description
ACSA	Airports Company South Africa
ACS	Access Control System
BCS	Background Check System
BDS	Behaviour Detection System
CCTV	Closed Circuit Television
GUI	Graphical User Interface
HMI	Human Machine Interface
IT	Information Technology
IISP	Intelligent Integrated Security Platform
PA	Panic Alarm
PIDS	Perimeter Intrusion Detection System
QMS	Queue Management System
RFI	Request for Information
RPAS	Remote Piloted Aircraft System
SIRS	Security Incidents Reporting System
SOW	Scope of Work / Statement of Work
VIDS	Vehicle Intrusion Detection System
WPO	Western Precinct Office
AVSEC	Aviation
ICAO	

Table 1 Glossary and Abbreviations

Definitions	Description
Cluster	Refers to a grouping of airports. Cluster 1 (JNB, BFN), Cluster 2 (CPT, UTN, GRJ, KIM) and Cluster 3 (DUR, PLZ, ELS).
Operator	Command center and Security control room Security Systems user.
Security Command Center	Command center refers to: a central place for security systems management. It carries out supervisory tasks and integrates all systems from airports and ACSA facilities. This is also a central place for crisis management.
Security Control Room	Airport alarms management center
Intelligent Integrated Security Platform	Refers to a single platform where all ACSA security systems are integrated and reports alarms, events, audio and data in real-time. It is also where security systems are managed through a single user interface.

Table 2: Glossary Definitions

TABLE OF CONTENTS

TABLES

1 INTRODUCTION

1.1 PURPOSE

Airports Company South Africa SOC Ltd hereby invites proposal for the supply, installation, commissioning, testing and support of an Intelligent Integrated Security Platform system for the period of 5 years (60 months).

1.2 OBJECTIVE

The objective of this procurement is to obtain a technology solution that must add value to ACSA's existing security services and take into account its existing system architecture. The solution must support the following strategic objectives:

- Improve efficiencies and incident response rates;
- Digitisation and automation of ACSA airports and facilities' security systems;
- Cost optimisation;
- Efficient allocation of people resources;
- Drive higher levels of security;
- Improve the safety and security of people, assets and information;
- Centralise security data and information;
- Reach set security level targets;
- Optimise existing system architecture;
- Increase the threat response rate;
- Improve the quality of security data and information (accuracy, timeliness, completeness and relevance);
- Improve overall awareness of any situation or current status of the airport;
- Improve business continuity;
- Increase the confidence level of employees, at all levels, to respond accurately to potential security breaches;
- Improve management decision making; and
- Design and implement solutions with potential commercial value.

1.3 BACKGROUND

Airport security provides an environment wherein passengers, staff, aircraft, and airport property are given assurance and protection from accidental or malicious harm, crime, terrorism and other unlawful acts. Evolution of airport security environments and rapid technological advancement has in recent years highlighted the need for airports around the world to develop and co-ordinate their security systems and functions into well-managed and streamlined operations. Effective airport security management involves far more than having the right security systems in place - it requires systems to be integrated and services to be continually updated and managed from centralised locations.

As noted by the South African Civil Aviation Authority (SACAA), “the primary objective of international civil aviation security is to ensure the protection and safeguarding of passengers, crew, ground personnel, the general public, aircraft and facilities of an airport serving international civil aviation, against acts of unlawful interference perpetrated on the ground or in-flight”. In response to the risk posed by these threats, Airports Company South Africa (ACSA) has deployed various security systems and techniques, such as access control and closed-circuit television, to ensure the safety of its airports. These systems currently operate independently of each other and are not integrated on a single platform. In addition, the lack of integration has resulted in suboptimal utilisation of the existing infrastructure.

An Integrated Security Management System (ISMS) will link individual systems and enable central operation from one application. Combining data from different sources will make systems more intelligent and, therefore, more effective. It is for these reasons that the Enterprise Security (ES) and Information Technology (IT) divisions embarked on a feasibility study to evaluate the viability of integrating ACSA’s security technologies onto a single platform. To this end, a Request for Information (RFI) was issued to the market in April 2021. The feedback from the RFI has indicated that ACSA stands to benefit significantly from the integration of its security systems. The available platforms in the market are scalable and will also enable the integration of future technologies that ACSA is currently evaluating. It is envisioned that the implementation of an integration solution will assist the organisation in managing its security resources (“boots on the ground”) in a much more coordinated and efficient manner which will drive down operating expenditure. The platform will also improve the monitoring and reporting of security-related incidents and allow for the consolidation of security processes.

2 SCOPE

The following sections consist of requirements that are in scope to detect, recover and respond.

2.1 IN SCOPE

2.1.1 FUNCTIONAL REQUIREMENTS

The following are considered an integral part of business needs that are going to be enabled by Intelligent Integrated Security Platform.

ID	FUNCTIONAL REQUIREMENT
BR1	**Provide an Intelligent Integrated Security System Design Architecture**
BR1.1	Delivers integrated intelligent security services
BR1.2	Considers the current environment and leverages existing security systems
BR1.3	Complies to regulatory statues such as POPIA, ICAO, CAA
BR1.4	Confirms to open standard protocols
BR1.5	Centralise administration and storage of data
BR1.6	Geographical mapping of areas
BR1.7	Provide Situational analysis or a heat map of high risk or high activity zones
BR1.8	Automation and Digitalisation of standard operating procedures against predetermined policies and business rules a) In line with International Civil Aviation Organisation (ICAO), AVSEC standards and guidelines
BR2	**Graphical User Interface** a) Operator must be able to read and write to any of the security systems from the integrated module, e.g. acknowledge, reset and escalate alarms through the GUI b) The solution GUI should be capable of utilising drawings and maps that are 3D and 2D. Bidder should consider and include all airport building layout drawings to be presented in 3D and perimeter barriers in 2D. c) The GUI should be capable of being driven via a touch screen interface.
BR3	**Cybersecurity**

	a) The IISP platform must also integrate network monitoring tools or software to detect any abnormalities and intrusions on the security system network. b) List our current cybersecurity system to integrate: a. SIEM Integration to the Intelligence Integrated Security Platform is not limited to the above-mentioned listed ACSA cybersecurity systems.
BR4	**External User Interface** a) The system must be able to provide different user interface view capabilities. The system should provide configurable user interface views for airports, clusters and command centre levels
BR5	**Operating Environment** a) Distributed Integrated platform. A single integration module should be able to operate all security system data/information that is spread across the airport level, cluster level and command centre level / WPO (Western Precinct Office) b) Completely scalable model from user/single site to Enterprise version covering multiples airports control rooms across the airports, cluster and centralised command centre. c) A multi-tiered hierarchy (as a federation system) centralises total control but allows individual sites and clusters to maintain control. d) Control rooms designs (considering cluster), video wall (for projected view), operator works stations and operator function designs.
BR6	**Redundancy** (a) Integrating module must have redundancy, and in the event of primary module technical failure, it must failover to a secondary or equivalent module to prevent any disruption of system operation and maintain continuity of service (b) All regional airports operating from the cluster shall be equipped with a client station for redundancy in an event network/communication to the main cluster is lost; and (c) The response must include diagrams to describe how the redundancy will work. (d) Scalable redundancy, whereby any workstation/server can be automatically promoted to being the primary host to connect with a single sub-system or multiple systems.
BR7	**Infrastructure Specification** • The Service Provider must provide the following infrastructure specifications for their system to function optimally: • Servers (CPU, RAM, HDD);

	• Storage (any additional storage required); • Network (e.g., ports to be opened, the bandwidth required for the solution to work optimally); and • Database (ACSA database standard is Microsoft SQL and Oracle). • IT Infrastructure Standards included in Annexure D • ICT Infrastructure hardware equipment that is provisioned from the appointed Service Provider must ensure that all warranties and maintenance agreements of such hardware equipment should be transferred to ACSA's current maintenance contractor • ICT Infrastructure or hardware provisioned and procured through the main contractor should include a three year onsite replace/fix warranty of: ○ 4 hours for low priority workloads/services ○ 8 hours for low priority workloads/services ○ next day for low priority workloads/services
BR8	(a) Solution Architecture Requirements • Architecture diagram(s); • Solution components (Application, Database, Supporting Technologies). A write up of each component is required; • Integration components (how the solution integrates with other solutions); • Information on what protocols and interfaces are supported; • An overview of the software, hardware and infrastructure components utilised in delivering the proposed Intelligent Integrated Security solution. This should include product names, specific modules utilised, integration, methods of user interface, reporting tools and references to any third-party products utilised; • Solution interactions with other systems and the data or messages that flow (flow diagrams); • Logical components of the solution and describe the basic domain functionality managed by that component; • Physical layout of the solution across hardware, servers, protocols and network devices; • Data movement between components and between external entities and application components; • List all assumptions made in your proposed solution; • Information on how your system integrates in an airport context, including examples of how it has been implemented at an airport; • Indicate availability to conduct a system demo of the solution; and

	• Indicate the degree to which customisations are allowed on the system to cater for future business requirements.

Table 3: Functional Requirements

2.1.2 NON-FUNCTIONAL REQUIREMENTS

The following are non-functional requirements that the IISP system must meet.

ID	NON-FUNCTIONAL REQUIREMENT
BR1	**System Physical Location:** a) The system must be available to all ACSA employees and stakeholders in 9 airports including Corporate.
BR2	**Solution Performance (speed and accuracy):** a) Immediate response when working on the solution, i.e., not click and section and wait. b) The system must be able to handle volumes during peak times. c) The system must be able to cater for bandwidth constraints and geographically dispersed locations. d) Users in different sites must have the same experience with the solution.
BR3	**System Response** a) All alarms, events, data, audio and video streaming exchange on the integrated module must be in real-time
BR4	**Synchronisation** a) Ability to synchronise completed incidents to the server when online.
BR5	**Scalability** a) The system must cater for future growth. e.g., adding of new functions and/or users
BR6	**Usability** a) The system must be easy to use with minimal training. b) Ease-of-use requirements must address the factors that constitute capacity of the software; to be understood, learned, and used by its intended users. The system must be easy to

	learn and operated by users with minimal training. It must also conform to usability standards for the graphical user interface.
BR7	**Reliability & Availability (Days / Hours)** a) The system must be available 24/7. Past performance reports and / statistics need to be provided to this effect. b) The solution must cater for high availability, backups and disaster recovery.
BR8	**Security** a) The system must align with ACSA Information Security policy and standards (to be provided to the service provider prior to contract agreement). b) The system's Active Directory (User Authentication) must align with ACSA standards (to be provided to the Service Provider prior to contract agreement) c) The system must ensure that the data is transmitted in a non-readable format (encrypted) and has strong key management. The system must provide encryption capabilities for stored data to ensure that data at rest is protected. d) Ensure that there are SSL certificates signed by the commercial CA (certificate authority)
BR9	**User Access Rights** a) The system must allow for users and / role-based permissions to be configured in order to control what system features and data users can access.
BR10	**Repeated authentication failure** a) The solution must notify an administrator within one minute if it cannot verify the identity of any user in less than three attempts within one period. In addition, the system should hide unauthorised functionality to users according to their user profiles.
BR11	**Integrity** a) There must be a single source of truth in terms of data and calculations where applicable. b) The solution must protect its communications from unauthorised intentional corruption during transit, including communications between its users. It must also protect its persistent data from unauthorised intentional corruption.
BR12	**Privacy and data ownership** a) The system must comply with ACSA's Information Security policies and standards, including POPI Act (to be provided to the Service Provider prior to contract agreement) b) All data to remain the property of ACSA and be accessible to ACSA in a format that can be easily utilised.
BR13	**Audit Trail**

	a) There must be an audit trail of who created, updated, closed, and deleted (must be authorised by the super users) the record within the time and date stamp.
BR14	**Service Access** a) All functions must be accessible via laptops, desktops, tablets, and cellphones. b) Stakeholder management function must be accessible via laptop, desktop, mobile and tablet.
BR10	**Operational** a) Business hours are between 8 am and7 pm. However, the system availability must be 24/7.
BR11	**Business Continuity** a) The system must have an alternative way to ensure business continuity in cases where there is an unfortunate event of downtime. b) The system must be able to perform business functions during downtime, and the system must be synced with the activities that were taking place during the time the system was down. c) Disaster recovery instance of the solution must be at a separate physical location, at least 25 km from the production instance. The sites should have separate utility feeds, e.g., power, network etc. d) IT Service continuity strategy solution must align to the recovery time and point objectives identified by the ACSA SOC Ltd. The IT Service Continuity strategy will be provided to the Service Provider prior to the contract agreement). e) Periodically (i.e., at least once annually), through testing, should provide assurance to the ACSA SOC Ltd regarding the effectiveness and adequacy of the IT Service continuity strategy. f) Up-to-date business continuity plan that demonstrates your company’s continuity arrangements for operational disruptions.
BR12	**Local Support.** • First line support for the solution will be done by ACSA. Details to be articulated in the Service Contract between ACSA and the Service Provider.
BR13	**Look and Feel:** • The system or solution appearance and style should align with ACSA’s Corporate identity and branding
BR14	**Integration:** • The system must be able to integrate to the following existing applications:

	- All integration requirements will be defined and detailed as per ACSA’s Integrated Control Document Template as per Annexure C

2.2 OUT OF SCOPE

The requirements that are not explicitly defined in this scope of work.

3 CURRENT SYSTEM OVERVIEW

3.1 CURRENT ENTERPRISE SECURITY LANDSCAPE

3.1.1 OVERVIEW

The diagram below illustrates the current security system landscape which is based on a variety of disparate systems

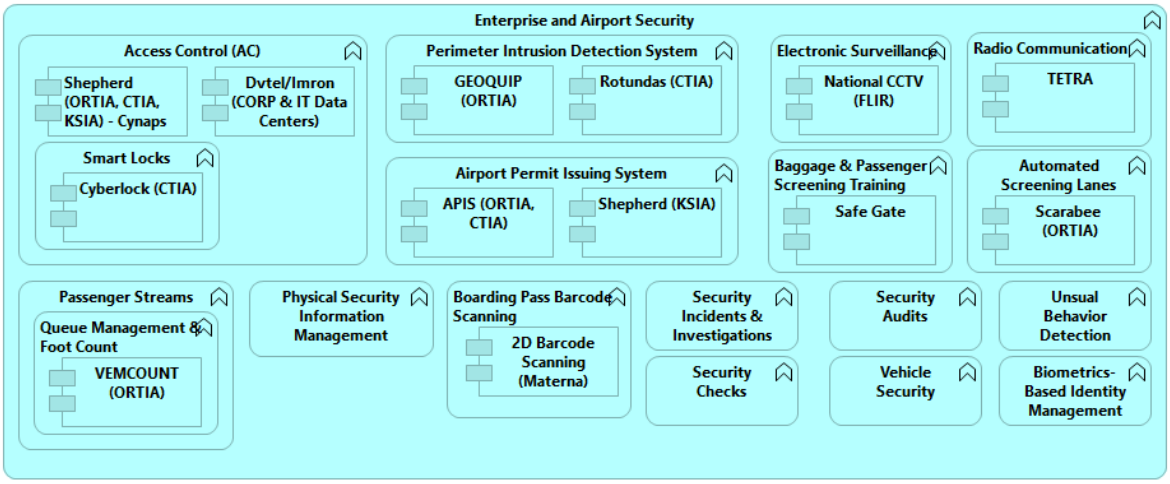
Enterprise and Airport Security
Access Control (AC)
Shepherd (ORTIA, CTIA, KSIA) - Cynaps
Dvtel/Imron (CORP & IT Data Centers)
Smart Locks
Cyberlock (CTIA)
Perimeter Intrusion Detection System
GEOQUIP (ORTIA)
Rotundas (CTIA)
Airport Permit Issuing System
APIS (ORTIA, CTIA)
Shepherd (KSIA)
Electronic Surveillance
National CCTV (FLIR)
Radio Communication
TETRA
Baggage & Passenger Screening Training
Safe Gate
Automated Screening Lanes
Scarabee (ORTIA)
Passenger Streams
Queue Management & Foot Count
VEMCOUNT (ORTIA)
Physical Security Information Management
Boarding Pass Barcode Scanning
2D Barcode Scanning (Materna)
Security Incidents & Investigations
Security Checks
Security Audits
Vehicle Security
Unsual Behavior Detection
Biometrics-Based Identity Management

Figure 1: Current Enterprise Security Landscape

3.1.2 Access Control – system is used to limit access to a physical location

3.1.2.1 Shepherd (ORTIA, CTIA, KSIA) – Cynaps

3.1.2.1.1 Number of Access Control Doors KSIA - 393

3.1.2.1.2 Number of Access Control Doors CIA - 483

3.1.2.1.3 Number of Access Control Doors ORTIA – 818

3.1.2.2 Imron (CORP & IT Data Centers) - IMRON V 10.9.51 & IT Data Centers IMRON UNITY V 10.5.21

3.1.2.3 Smart Lock (CTIA)

3.1.2.4 Fire and Emergency Doors – Genesys Software V 2.6.4.8

3.1.2.5 Aircraft Gates and Emergency Gates

3.1.3 Perimeter Intrusion Detection System PIDS – system is used to detect the presence of an

intruder attempting to breach a perimeter

3.1.3.1 Geoquip (ORTIA) - Windows 2007 Software Version 6.22.0

3.1.3.2 Rotundas (CTIA) - Windows 2002 Software Version 5.20

3.1.4 Airport Permit Issuing System – system is used to issue permits which will grant access to users at the airport

3.1.4.1 APIS (ORTIA, CTIA)

3.1.4.2 Shepherd (KSIA)

3.1.5 CCTV – system is used to detect and deter criminal activities using electronic surveillance

3.1.5.1 FLIR All Sites Except CIA – V 8.0.0.6112

3.1.5.2 FLIR CIA – V 8.0.0.6113

- Number of ORTIA Cameras – 2845) \ FLIR Version 8.0.0.6112
- Number of PIDS Cameras – 89\ FLIR Version
- Number of CIA Cameras – 1802 FLIR Version 8.0.4.6125
- Number of KSIA Cameras – 933 FLIR Version 8.0.0.6112
- Number of PE Cameras-183 FLIR Version 8.0.0.6112
- Number of BFN Cameras -40 FLIR Version 8.0.0.6112
- Number of Cameras UPN -41 FLIR Version 8.0.0.6112
- Number of Cameras ELS -145 FLIR Version 8.0.0.6112
- Number of Cameras KIM -51 FLIR Version 8.0.0.6112
- Number of cameras GRG – 141 FLIR Version 8.0.0.6112
- Number of cameras Corporate -136 FLIR Version 8.0.0.6112

3.1.6 Terrestial Trunked Radio Communication - used to provide secure, reliable and instant voice and data communications in mission-critical, operations-critical and business-critical environments

3.1.6.1 TETRA ORTIA - Linux CentOS 7 Version 2.28.36.19521

- CIA - Linux CentOS 7 Version 2.28.24.14361
- KSIA Linux CentOS 7 Version: 2.28.24.14361
- GRJ Linux CentOS 7 Version: 2.28.36.19521
- ELS Linux CentOS 7 Version: 2.28.36.19521
- PLZ Linux CentOS 7 Version: 2.28.24.14361
- KIM Linux CentOS 7 Version: 2.28.24.14361
- BFN Linux CentOS 7 Version: 2.28.24.14361
- UTN Linux CentOS 7 Version: 2.28.24.14361

3.1.7 Queue Management System (QMS) - used to count the number of people entering and exiting the airport or a specific area

3.1.7.1 Queue Management & Foot Count – Vemcount Software Version 9.3.6

3.1.7.2 XOVIS Passenger Flow – ACSA Central Search Point Management – Custom Software

3.1.8 Passenger and Baggage Screening – used to scan passengers and baggage for compliance with airport restrictions

3.1.8.1 2D Barcode Scanning (Materna)

3.1.9 Automated Security Lanes - advanced security screening software that automatically identifies potential threats via live, interactive 3D imaging for analysis purposes

3.1.9.1 Scarabee (ORTIA)

3.1.10 Panic and Fire Alarms – used to alert law enforcement and first responders of Incidents

- ORTIA – 24
- ORTIA Cargo – 49
- BFN – 2
- KIM-14
- ELS-2
- KSIA – 32
- UPN -2
- GEORGE -8

3.1.11 Patrol Badging System

3.1.12 PA System – Bosch Praesideo System Software Version Dante 6.37.5943

3.1.13 Fleet Tracking System

3.1.14 Key Control System

3.1.15 Non-Security Solutions

3.1.15.1 Building Management - used to control and monitor the building's mechanical and electrical equipment such as ventilation, lighting, power systems, fire systems and security systems

3.1.15.1.1 IMCS/Rockwell

3.1.15.2 Airport Management System (AMS) - used to provide flight information

3.1.15.2.1 SITA AMS

3.1.15.3 Fire Detection System, ZP4 Panels

4 CONCEPTUAL DESIGN

4.1 OVERVIEW

The diagram below is a conceptual design of the Integrated Intelligent Security Platform. The platform will deliver a set of intelligent security services and link underlying airport security systems.

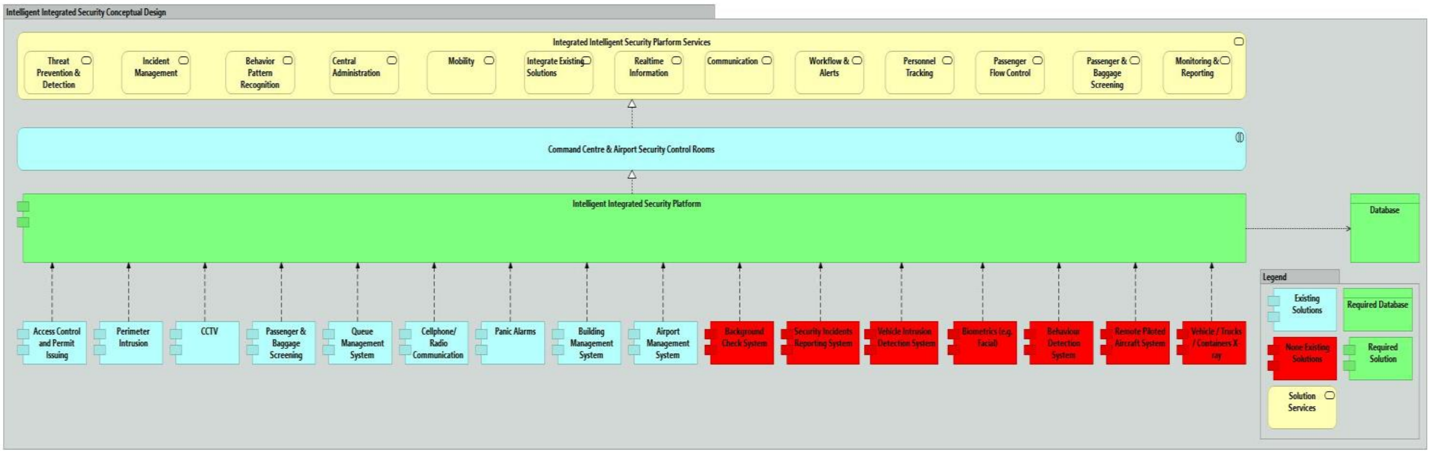
Intelligent Integrated Security Conceptual Design
Integrated Intelligent Security Plarform Services
Threat Prevention & Detection
Incident Management
Behavior Pattern Recognition
Central Administration
Mobility
Integrate Existing Solutions
Realtime Information
Communication
Workflow & Alerts
Personnel Tracking
Passenger Flow Control
Passenger & Baggage Screening
Monitoring & Reporting
Command Centre & Airport Security Control Rooms
Intelligent Integrated Security Platform
Database
Access Control and Permit Issuing
Perimeter Intrusion
CCTV
Passenger & Baggage Screening
Queue Management System
Cellphone/ Radio Communication
Panic Alarms
Building Management System
Airport Management System
Background Check System
Security Incidents Reporting System
Vehicle Intrusion Detection System
Biometrics (e.g. Facial)
Behaviour Detection System
Remote Piloted Aircraft System
Vehicle / Trucks / Containers X ray
Legend
Existing Solutions
Required Database
None Existing Solutions
Required Solution
Solution Services

Figure 2: Conceptual Design of the Integrated Intelligent Security Platform

4.1.1 Integrated Intelligent Security Services

4.1.1.1 Threat Prevention Security Services

4.1.1.2 Incident Management

4.1.1.3 Behaviour Pattern Recognition

4.1.1.4 Realtime Information

4.1.1.5 Central Administration

4.1.1.6 Central Database

4.1.1.7 Mobility

4.1.1.8 Integrate Existing Solutions

4.1.1.9 Workflow and Alerts

4.1.1.10 Communication

4.1.1.11 Passenger Flow Control

4.1.1.12 Personnel Tracking

4.1.1.13 Monitoring and Reporting

4.1.2 List of existing Systems

Below is a list of existing systems that need to be integrated with the intelligent integrated Security Platform:

4.1.2.1 Access control and permit issuing – Intention is to centralise and use one access control system across the organisation in future

4.1.2.2 Perimeter Intrusion Detection System – Intention is to centralise and use one access control system across the organisation in future

4.1.2.3 CCTV

4.1.2.4 Passenger and Baggage Screening Systems

4.1.2.5 Queue Management System

4.1.2.6 Terrestrial Trunked Radio Communication (TETRA)

4.1.2.7 Panic and Fire Alarms

4.1.2.8 Emergency and Fire Doors

4.1.2.9 Aircraft Gates and Emergency Gates

4.1.2.10 Patrol Badging System

4.1.2.11 Key Control System

4.1.2.12 Building Management System

4.1.2.13 Airport Management System

4.1.2.14 Smart Security Lanes

4.1.3 List of Future Systems

Below is a list of future systems that will be integrated with the intelligent integrated Security Platform:

4.1.3.1 Background Check System

4.1.3.2 Security Incidents Reporting System

4.1.3.3 Vehicle Intrusion Detection System

4.1.3.4 Biometrics (e.g. Facial & Finger)

4.1.3.5 Behaviour Detection System

4.1.3.6 Remote Piloted Aircraft System

4.1.3.7 Vehicle / Trucks / Containers X-ray

4.1.3.8 Watch list of wanted persons

4.1.3.9 Fleet Tracking System

5 PRICING

5.1 The Service Provider to provide ACSA with the solution pricing as per the below table for a period of five years.

5.2 Items that are not applicable should be highlighted as such

COST	
Requirements Gathering	R
System Design Architecture	R
Functional Design	R
Detail Design	R
Development for Integration	R
Implementation (incl. Project Management and other relevant resources)	R
Integration	R
Prototyping (approximately nine existing systems)	R
Quality Assurance	R
Testing (Unit, Functional, System)	R
Hardware (including network size and speed etc.)	R
Software (Licences)	R
Reporting	R
Support and Maintenance	R
Extended OEM Warranty for three years (Hardware and Software)	R
Contingency	R
TOTAL	**R**

6 SUPPORT AND MAINTENANCE

This section describes what Support and Maintenance entail in general and further describes what maintenance entails for ACSA.

ACSA requires the Support Services from a Service Provider as described below:

6.1.1 Day to day support activities performed to remediate/report on security incidents, alerts and threat logs generated by the system's internal monitoring;

6.1.2 The Service Provider will be required to respond to and remediate all incidents in line with ACSA vulnerability management process. All security incidents will be logged on the IT service desk systems (Service NOW); and

6.1.3 The response and remediation times depicted below must be adhered to. This will form part of the SLA's that will be agreed to between the Service Provider and ACSA.

6.2 DEFINITION OF INCIDENTS, PRIORITIES AND SLA's

Priority 1: Total system failure

Priority 2: Partial system failure with minimum monitoring functionality

Priority 3: Non-critical fault/failure logged at night or over the weekend. It has no impact on the operations of the airport

Priority 4: Minor incidents or move/change or installation of new item

6.3 INCIDENT MANAGEMENT RESPONSE AND RESOLUTION TIMES

Incident management response and remediation times for (Office Hours, After Hours, Weekends and Public Holidays)			
	Response	**Restoration**	**Update Feedback**
P1	15min	1hrs	30min
P2	30min	4hrs	1hr
P3	2hrs	8hrs	2hrs
P4	4hours	24hrs	8hrs

Table 4: Incident Response and Remediation Time

6.4 INCIDENT LOGGING PROCEDURE

ACSA requires the Service Provider to adhere to the following incident logging procedure:

6.4.1 All security incidents must be logged with ACSA service desk via email, telephone or on the self-service web portal. The incident status must be updated regularly depending on the priority of the incidents until resolution;

6.4.2 All security incidents must be updated with a detailed resolution before closure. The Service Provider must notify the service desk immediately on resolution of the incident.

6.5 IMPLEMENTATION SLAs

6.5.1 The implementation schedule (dates, milestones, success criteria etc.) will be defined in the project kick off meeting. Should such schedule not be agreed to, it is stated that there is no consensus and/or the parties, and this affects the validity of the contract.

6.5.2 The approved minutes of the kick-off meeting will serve as the agreement by the parties of the service level and penalties.

6.5.3 The approved minutes from the kick-off meeting shall be regarded as an Appendix and form part of this agreement

6.5.4 Where the Service Provider does not meet the implementation dates as documented and agreed by both parties in the kick-off meeting, unless clearly and timeously communicated in writing and the schedule re-baselined by the ACSA project manager, ACSA will notify the Service Provider of breach of service.

6.5.5 The service provider is expected to deliver this project in line with the agreed timelines, milestones and conditions.

6.5.6 The Supplier must propose how to best group features and provide incremental solution design, development, testing and release plan.

6.5.7 For each release that misses the scheduled release date, and or is above SIT to UAT defect leakage tolerance, ACSA will withhold 10% of the implementation fee per such release. Defect leakage from SIT to UAT must be less than 10% tolerance limit.

6.5.8 The solution must be in early life support for a minimum of four (4) months**.**

6.6 BREACH AND PENALTIES

As detailed in the next sections, the following penalties shall apply in the event of a breach of service levels as agreed. The service provider shall restore the solution that is in scope within times specified in the service level agreement; the following project and operational-based penalties shall apply for failing to deliver the expected milestone or restore the services within agreed timelines:

SLA Breach	Penalty
Project SLA Breach & Penalties	
If the project milestone or release misses the scheduled release date and or is above SIT to UAT defect leakage tolerance	10% of the implementation fee per such release will be withheld.
Operational SLA Breach & Penalties	
P1 Incidents are resolved within one hour after SLA time lapsed for two consecutive times in one month across any of the sites in scope	20% of the monthly fee will be deducted per invoice and up to 60% in one contractual year. After that, termination procedures will be implemented.
Incidents are resolved within two hours and beyond after SLA time lapsed for three consecutive times in one month across any of the sites in scope	30% of the monthly fee will be deducted and up to 60% in one contractual year. After that, termination procedures will be implemented.
If a Service Provider misses Incident Management SLAs in any three consecutive months across any sites in scope	50% of the monthly fee will be deducted.
If a Service Provider misses Incident Management SLA's consecutive in any 4 months across all site's ins cope – will be deemed as a material breach, and the contract will be referred for performance management and termination procedures	50% of the monthly fee will be deducted.
Five or more missed SLAs across all sites in scope on or across Acquisition Management, IMACDs; Asset Management; Configuration Management; Maintenance and Repair in a measuring period	20% of the monthly fee will be deducted per invoice

Table 5: SLA breaches and penalty for incidents

Failure to perform maintenance and/or services in accordance with the scheduled dates or Priority list and SLA agreements shall result in the following penalties:

Maintenance	**Penalty**
Maintenance not done or proof of carrying maintenance out not submitted.	No payment of invoice.

Table 6: Failure to provide maintenance

7 REPORTING

(a) As part of ongoing performance management, ACSA requires that the Service Provider provides the following reports as contained in the table below. These reports will be presented to ACSA on demand and during implementation and ongoing support of the services.

(b) ACSA reserves a right to change a list of reports as requested and will review these on a regular basis, and such changes should not attract additional costs.

(c) The project meetings will be held weekly, and/or on-demand for the duration of the contract and arranged by the ACSA Information Security team to discuss the following, but not limited to:

7.1 WEEKLY AND MONTHLY REPORTS

#	Report Name	Frequency	Content and Format	Submitted to
1	Service Request Status (not incidents)	Every day of the week and a consolidated version for all 4 weeks on the last day of the month-end	Status of new enhancements, fixes, requests	IT Airport Systems
2	Weekly Service Review Reports for open, closed incidents, the status of each incident in terms of SLA.	Every day of the week and a consolidated version for all 4 weeks on the last day of the month-end.	Open and closed incidents. Status of each incident in terms of SLA. Reason for SLA breaches, if any and measures that will be put in place to avoid a breach.	IT Airport Systems

#	Report Name	Frequency	Content and Format	Submitted to
3	Maintenance reports: report against the maintenance schedule. This will include issues picked up during their maintenance.	Every day of the week and a consolidated version for all 4 weeks on the last day of the month-end	Modules worked on. Issues discovered per module and how they were resolved. Details on any general maintenance work carried out.	Airport System and Enterprise Security Team
4	Monthly Systems Availability Report against the ACSA required target of 99.9 % uptime.	Last day of the month	System availability System downtime	Airport System and Enterprise Security Team
5	Preventative work done.	Monthly (i.e., 4th of the following month).	Report on various preventative work as per section 4.2 above.	Airport System and Enterprise Security Team
6	Issues for ACSA's attention.	Last day of the month	Any relevant issues that need to be brought to ACSA's attention by the Service Provider.	Airport System and Enterprise Security Team
7	Ad-hoc	As and when required	Ad-hoc, depending on the request at hand.	Airport System and Enterprise Security Team

Table 6: Reporting Matrix

7.2 MEETINGS

As part of ongoing performance management and project delivery, ACSA requires that the Service Provider attend monthly and weekly meetings.

Frequency	Meeting Name	Standing Agenda	Participants and Role	Prior documents to be submitted by the Service Provider	Documents to be produced after meeting
Monthly	Project Board Meeting	Discuss all aspects of Monthly reports Discuss Project Costs, Timeline, Risks, Issues, Resources, etc. Discuss all deliverables produced to trace successful delivery on Business Requirements.	IT PMO, Service Provider's Service Delivery Manager, ACSA contract owner, ACSA Technical Lead, Project Sponsor, Other Stakeholders per Invitation	Project Board Pack including Planned Presentation. Previous meeting action items Monthly Reports.	Attendance Register Meeting action items
Weekly	Progress Meeting	Progress Reporting, Performance Management, Security Posture, Security Incidents/Threats Reporting, Exception Reports, Risk Register, Areas of Focus, discuss	Service Provider's Service Delivery Manager, Technical Resources and ACSA Security team	Minutes of Previous Meeting. Updated Risk and Issue Log.	Attendance Register. Meeting action items Acceptance of deliverables.

Frequency	Meeting Name	Standing Agenda	Participants and Role	Prior documents to be submitted by the Service Provider	Documents to be produced after meeting
		high-level service deliverables/milestones, Timelines and delivery, Environment Risks / Issues / Assumptions, Contractual/Financial and Governance, General and all other requirements related to the services. Internal and External Audits of the Services in Scope.			
Ad-hoc	Ad-hoc	Ad-hoc	Stakeholders as and when required	Ad-hoc	As agreed by all parties
Monthly	Operational Meetings	Review system operations, vendor performance	Service provider & IT Operations Department	Operational reports	Minutes, attendance register.

Table 7: Meetings Matrix

8 DOCUMENTATION

The following project-related documentation must be produced by the Service Provider during the implementation of the project:

- Project Management deliverables as per ACSA standards
- Architectural Design
- Functional Specification
- Technical Specification
- Interface Control Document
- Quality Assurance Specific Documentation (Test plan, Test cases, Test results for different types of solution testing (unit, functional, performance, stress, vulnerability), List of Defects)
- Operational Manuals
- Training Manuals

9 SOLUTION GUIDELINES

- The solution must provide the functions and services required to support the business capability.
- There should be a single application to support a given business capability, i.e., the solution must not re-implement a capability already available in the portfolio unless it is replacing the current one.
- The solution must be as secure as business requirements dictate.
- The solution must meet legal and conformance requirements, including those for privacy.
- The solution must provide adequate performance and responsiveness.
- The solution must be able to scale, without redevelopment, for anticipated increase in volumes for the next five years.
- The solution must be reliable and easily recoverable.
- The solution must validate input data and maintain the integrity of any data added, updated or exported.
- The solution must provide APIs which allow services to be accessed via an interface conforming to industry standards adopted by ACSA, e.g., Web Service (REST, SOAP).
- The solution must avoid “hard coding” of value, i.e., any variables which are likely to change must be externalised to the database or parameter/rule files
- The solution must trap errors and report them in a meaningful and persistent way
- The solution end-user interfaces must be intuitive and standards-based to facilitate ease of adoption and reliable usage as well as reduced training requirements.
- The solution must be documented to a standard that facilitates:
- Ese of installation and configuration.
- Ease of operation by end-users.
- Easy problem determination and resolution.
- Impact analysis for change requests.

- Ease of adaptation when required; and
- The solution must not expose ACSA to undue risk.

10 APPROVALS

This document will be approved by the following TPEC members:

____

Tshepo Mobu **Date:**

Designation: IT Technical Assistance

____

Susu Makhuvha **Date:**

Designation: Compliance Specialist

____

Frans Mohlabeng **Date:**

Designation: Assistant Manager Aviation Security Operations