RFB NUMBER: SACU/017/2026/PB

Replacement of the Access Control and Surveillance System at the SACU Secretariat HQ Building

CLOSING DATE & TIME

Friday, 31 October 2025 at 17H00

POSTAL & PHYSICAL ADDRESS FOR BID SUBMISSION

Southern African Customs Union (SACU) - Secretariat
Private Bag 13285
Corner Julius K. Nyerere and Sir Seretse Khama Street
Windhoek, Namibia, 9000

COMMERCIAL ENQUIRIES

Mr. Hermanus L. Esterhuizen
Procurement Officer
Tel: +264 (61) 295-8000/37
Fax: +264 (61) 245 611
Email: Leon.Esterhuizen@sacu.int

TECHNICAL ENQUIRIES

Mr. James Shipena
Facilities and Administration Officer
Tel: +264 (61) 295-8000/45
Fax: +264 (61) 245 611
Email: James.Shipena@sacu.int

Submit one (1) Electronic Bid to: procurement@sacu.int

TABLE OF CONTENTS

1. INTRODUCTION 1
2. OBJECTIVES 1
3. SCOPE OF WORKS 1
4. OVERVIEW OF THE EXISTING ACCESS CONTROL AND SURVEILLANCE SYSTEM 2
5. TARGET SYSTEM REQUIREMENTS 3
6. SOLUTION DELIVERY AND COMMISSIONING 6
7. MAINTENANCE AND SUPPORT 8
8. TECHNICAL SOLUTION SPECIFICATION 8
9. METHODOLOGY 9
10. DELIVERABLES AND PAYMENT MILESTONES 10
11. EXPERTISE REQUIRED 10
12. SUBMISSION OF BIDS 11
13. EVALUATION OF BIDS & AWARD CRITERIA 11
14. PRIME CONTRACTOR RELATIONSHIP 13
15. FINANCIAL ARRANGEMENT 13
16. CONFIDENTIALITY 14
17. OWNERSHIP OF BIDS 14
18. MODIFICATION OF TERMS 14
19. CONTRACT ADMINISTRATION 14
20. BID FORMAT 15
21. DOCUMENTATION CHECKLIST 19

APPENDIX A – FORMAT OF THE PROPOSAL 17
APPENDIX B – FORMAT OF THE LETTER OF INTRODUCTION 20

APPENDIX A – FORMAT OF THE PROPOSAL 17
APPENDIX B – FORMAT OF THE LETTER OF INTRODUCTION 20

1. INTRODUCTION

1.1 The Southern African Customs Union (SACU) consists of five Member States, namely Botswana, Eswatini, Lesotho, Namibia and South Africa. The SACU Secretariat (Secretariat) was established in 2004 to administer and coordinate the activities of SACU institutions. More information is available on SACU's website (http://www.sacu.int).

1.2 The Secretariat intends to modernise its physical security infrastructure by replacing the existing legacy system with a unified, biometric-based Access Control and Video Surveillance System at the SACU Headquarters located in Windhoek, Namibia. To this end, the Secretariat invites suitably qualified vendors to supply, install, and commission a standards-compliant access control system, along with accompanying biometric hardware, surveillance devices, and centralised management software.

2. OBJECTIVES

2.1 The objectives of this project are to:

(a) replace the Secretariat's existing legacy access control system with a modern, scalable, and biometrically secure platform;

(b) strengthen system governance by improving administrative authentication and introducing structured, role-based control over configuration and user management functions;

(c) enhance the reliability and resilience of the access control and surveillance infrastructure through improved backup and recovery mechanisms;

(d) integrate physical access with real-time surveillance monitoring and event recording to support effective incident response and investigation;

(e) improve the overall security posture by enabling zone-based access management, intelligent alarms, and real-time notifications for abnormal activity; and

(f) deploy a centrally managed solution that is compliant with international standards and capable of running either fully on-premises or in a hybrid cloud environment, in alignment with the Secretariat's ICT strategy.

3. SCOPE OF WORKS

3.1 The appointed service provider shall be responsible for the supply, installation, configuration and commissioning of a modern Access Control and Surveillance System at the SACU Secretariat premises in Windhoek, Namibia. The scope shall include, but not be limited to, the following:

(a) conduct a site audit to assess the current environment, identify infrastructure to be replaced, and confirm layout for new access points and surveillance coverage zones;

(b) supply and install all required biometric access hardware, IP-based surveillance cameras, access controllers, cabling and networked peripherals;

(c) deploy and configure the central management software to support role-based administration, zone-level access control, surveillance integration and alarm monitoring;

(d) integrate the access control system with real-time video surveillance, ensuring linkage between access attempts and event-triggered footage;

(e) ensure the system is capable of operating in either a fully on-premises model or a hybrid-cloud environment, with local autonomy at the device level in the event of network interruptions;

(f) support initial deployment for 50 users and 20 access points, with configuration flexibility for seamless scaling to at least 100 users and 50 access points as future needs arise;

(g) implement alarm and notification workflows for abnormal access behaviour (e.g. unauthorised attempts, forced door entries, device tampering);

(h) set up audit logging, reporting dashboards and secure data retention policies to support compliance and internal reviews; and

(i) ensure a structured handover process, including baseline configuration documentation, administrator training and operational readiness verification.

4. OVERVIEW OF THE EXISTING ACCESS CONTROL AND SURVEILLANCE SYSTEM

4.1 The current Access Control and Surveillance System is a legacy implementation composed of multiple discrete components with limited interoperability, administrative control, and resilience.

4.2 The system includes the following:

(a) **UNIS Access Control Software**: used as the administrative front-end for managing user credentials, access zones and authentication policies. This is operated from a dedicated workstation located in the Security Control Room;

(b) **Biometric Access Terminals**: a mix of Virdi fingerprint/card readers installed at various secure entry points. These devices support both biometric and proximity card authentication and are integrated with the UNIS platform;

(c) **Surveillance Camera Infrastructure:** comprising the following components:

(i) indoor and semi-outdoor **Vivotek 720p HD WDR Pro** dome cameras positioned throughout the facility for standard surveillance coverage; and

(ii) **weatherproof Vivotek IP67-rated cameras** used at exterior or exposed locations, designed to withstand harsh conditions and provide consistent image quality;

(d) **Video Management and Recording**: comprising of the following components:

(i) a **network video recorder (NVR) device** used for capturing, storing, and retrieving surveillance footage; and

(ii) **video management software (iVMS)** operated by security personnel for live monitoring and playback;

(e) **Monitoring and Display Infrastructure:** Display monitors and workstations are positioned in the Security Control Room to support continuous live surveillance viewing and access control administration. These include operator terminals used to interface with the video management system; and

(f) **Application Hosting Infrastructure:** comprising of the following:

(i) a standalone physical server used to host the access control and surveillance applications; and

(ii) a dedicated, closed-loop network interconnects biometric devices, surveillance cameras, video management systems and monitoring workstations. This network operates independently of SACU's enterprise ICT environment.

5. TARGET SYSTEM REQUIREMENTS

5.1 The SACU Secretariat seeks a robust, fully integrated Access Control and Surveillance Solution to modernise its physical security posture, improve administrative efficiency, and ensure long-term operational reliability. The solution must meet the following minimum technical, functional and architectural specifications.

5.2 **Access Control Requirements**

(a) The system shall support biometric fingerprint and proximity card authentication at all access-controlled entry and exit points, ensuring multi-factor authentication capabilities.

(b) A centralised administrative interface must allow designated administrators to define, assign, and revoke user access rights based on roles and responsibilities.

(c) The system must support configurable access zones such as restricted areas, open zones, and temporary permissions, with the ability to define time-based access rules, including working hours or shift patterns.

(d) All access attempts, whether granted or denied, must be logged in real time and retained in an audit-ready format for administrative and security review.

(e) The system must trigger alerts for unauthorized access attempts, forced entries, terminal tampering, or repeated authentication failures.

(f) Access events must be time-synchronized with surveillance footage to support incident review and investigation.

5.3 Video Surveillance Requirements

(a) All deployed cameras must offer a minimum resolution of 1080p (Full HD), with wide dynamic range for high-contrast environments and night vision for low-light conditions.

(b) The system must provide comprehensive surveillance coverage for both internal spaces and outdoor or perimeter zones, with weatherproof IP-rated camera models for exterior deployment.

(c) Motion detection must be supported to trigger event-based recording and optimise storage capacity, with per-camera configuration options available to administrators.

(d) Surveillance footage must be stored securely in a tamper-resistant format, with configurable retention periods and an intuitive interface for search and export.

(e) The system must include a centralized video management platform that supports live viewing, multi-channel playback, incident tagging, and role-specific access permissions.

(f) Video and access control data must be linked through timestamps or analytics to enable comprehensive event correlation and response.

(g) The system must have functionality for maintaining activity logs of administrative users as well as the logs for the movement in and out of various locations within the SACU premises.

5.4 System Architecture and Hosting

(a) The system must support on-premises hosting and provide compatibility with hybrid-cloud deployment models if needed.

(b) Where a dedicated standalone infrastructure is proposed or retained, the supplier shall be responsible for facilitating secure connectivity to SACU's internal network to enable internet access and centralised data backup services.

(c) System devices, such as access terminals and cameras, must be capable of autonomous operation during network outages, with events automatically synchronised when connectivity is restored.

(d) All components must be compatible with SACU's existing virtualised infrastructure or include standalone hardware where appropriate.

(e) Communication between system components must be protected using secure encrypted channels, with centralised enforcement of access control policies to prevent unauthorised access or modification.

5.5 Scalability and Integration

(a) The system must support a minimum of 50 users and 20 access-controlled points on initial deployment, with the ability to scale to 100 users and 50 access points through configuration or licensing adjustments.

(b) The system must support open standards such as ONVIF for surveillance integration, and provide directory-level compatibility where applicable, such as integration with Active Directory for managing user access profiles.

(c) Selected existing SACU infrastructure, including compatible surveillance cameras, display monitors, or cabling, may be reused subject to technical validation during the site audit.

5.6 Monitoring and Reporting

(a) The system must provide web-based or locally hosted dashboards for real-time monitoring of access activity, surveillance feeds, and overall system health.

(b) It must generate comprehensive audit logs capturing access events, user activity, system changes, and hardware alerts in a secure and exportable format.

(c) Reporting capabilities must allow for both standard and customised reports, covering areas such as access trends, incident analysis, and system diagnostics, with output in formats like PDF and Excel.

5.7 Serviceability and Maintenance

(a) The system must allow administrators to perform remote diagnostics, apply updates, and configure system parameters through secure management tools.

(b) Diagnostic features must alert staff to device malfunctions, disconnections, or misconfigurations with real-time notifications.

(c) The supplier shall deliver user training, system documentation, and first-line support resources to support SACU's ongoing internal maintenance.

(d) Features for system backup, restoration, and configuration replication must be included to ensure resilience and continuity in case of failure or data loss.

6. SOLUTION DELIVERY AND COMMISSIONING

6.1 The appointed supplier shall be responsible for delivering a complete and operational Access Control and Surveillance Solution at the SACU Secretariat. This includes the installation, integration, testing, training, documentation, handover, and post-implementation support of the system.

6.2 Supply, Delivery and Installation

(a) The supplier must supply, install, and physically commission all approved system components, including biometric terminals, surveillance cameras, servers, controllers, network infrastructure, and monitoring workstations.

(b) Software components must be installed and configured to SACU's specifications, including access control rules, video management, role-based permissions, backup protocols, and event handling workflows.

(c) The supplier is expected to integrate all new components into a cohesive, centrally administered platform and, where applicable, interface with retained existing devices identified during the site audit.

6.3 System Testing and Quality Assurance

(a) A full end-to-end system test must be conducted to validate access logic, camera visibility, system performance, alerts, logs, and user interaction flows.

(b) The supplier shall engage SACU stakeholders in user acceptance testing, guided by a documented test plan, and resolve all issues before formal sign-off.

6.4 Training and Knowledge Transfer

(a) Practical training must be delivered to both System Administrators and Security Officers, covering core system operation, user and access management, video monitoring, alert handling, and maintenance tasks.

(b) User training shall include procedures for registration, authentication protocols, and proper usage at access points.

(c) Training materials and reference guides must be supplied in printed and digital formats.

6.5 Documentation and Manuals

(a) The supplier shall provide full system documentation, including:

(i) architectural layout and system design

(ii) administrator and operator user manuals

(iii) configuration settings and credentials handover

(iv) maintenance procedures, escalation paths, and support contacts

(b) All documentation must be specific to the SACU environment and accurately reflect the installed configuration.

6.6 Handover and Commissioning

(a) Upon completion of installation, configuration, and testing, the supplier shall formally hand over the commissioned system to SACU.

(b) The system must be fully operational, meet all technical requirements, and be ready for production use.

(c) A commissioning report shall accompany the handover, documenting component functionality, user access provisioning, and final administrator credentials.

6.7 Warranty

(a) The supplier shall provide a 30-day workmanship and installation warranty commencing from the date of successful system commissioning. This warranty shall cover all configuration errors, installation defects, and functional issues arising from the implementation process.

(b) In addition, all hardware and licensed software components supplied as part of the new system must be covered by the respective original equipment manufacturer (OEM) warranties, including biometric devices, surveillance cameras, controllers, servers, and software licenses. Warranty coverage

shall not extend to existing SACU equipment that has been integrated into the solution.

7. MAINTENANCE AND SUPPORT

7.1 Following the expiry of the installation warranty, the SACU Secretariat may, at its discretion, enter into a formal Maintenance and Support Agreement with the appointed supplier to ensure the continued performance, availability, and security of the Access Control and Surveillance Solution.

7.2 Bidders are encouraged to propose an optional annual Service Level Agreement (SLA) as part of their submission, covering aspects such as on-site support, critical component replacement timelines, and extended service hours.

7.3 SLA proposals should clearly define service tiers, coverage inclusions and exclusions, escalation paths, and pricing applicable to SACU's environment beyond the warranty period.

8. TECHNICAL SOLUTION SPECIFICATION

8.1 Bidders are required to submit a detailed and structured technical proposal describing the architecture, components, and operational model of their proposed Access Control and Surveillance Solution. The proposal must demonstrate how the solution meets or exceeds **SACU's Target System Requirements** defined in **Chapter 5.**

8.2 **Proposal Structure and Supporting Material**

(a) The proposal must include comprehensive technical specifications for all key components, including biometric authentication devices, access control units, surveillance cameras, management consoles, and associated software platforms.

(b) The technical submission should clearly explain system modularity, resilience, upgradeability, data protection mechanisms, and approaches for high availability.

(c) Bids must clearly identify:

(i) all new equipment to be supplied, specifying the make and model of each component;

(ii) the existing SACU-owned equipment proposed for reuse, including its functional role in the overall solution; and

(iii) the extent of proposed reuse. Higher levels of appropriate reuse of SACU's existing equipment will be viewed more favourably during evaluation, provided compatibility and performance are not compromised.

(d) Proposals accompanied by architecture diagrams, process flowcharts, infrastructure layouts, and system topology maps will be evaluated more favourably.

8.3 Integration and Reuse of Existing Infrastructure

(a) The proposal must describe how the proposed solution will integrate with SACU's existing digital and physical infrastructure, including but not limited to retained surveillance cameras, cabling, power supplies, wall brackets, and directory services such as Active Directory.

(b) Where reuse is proposed, bidders must describe compatibility assumptions and any required interfaces, converters, or adjustments to ensure performance and stability.

8.4 Bill of Materials and Warranty Details

(a) Bidders must provide a detailed Schedule of Materials listing all hardware, accessories, and software licenses to be supplied.

(b) The schedule must include the item description, quantity, manufacturer and model, and OEM warranty duration associated with each item.

(c) This schedule must form part of the pricing and technical submission.

8.5 Component Sourcing and Dependencies

(a) Bidders must identify all third-party technologies and services embedded in the proposed solution, including OEM providers, platform vendors, and licensing tiers.

(b) Any use of proprietary SDKs, cloud APIs, or third-party monitoring tools must be declared with associated dependencies and ongoing costs.

(c) The proposal must also confirm whether the solution includes integration with retained infrastructure, and if so, any interoperability limitations must be disclosed.

9. METHODOLOGY

9.1 Bidders must submit a concise and practical description of the methodology they intend to apply in implementing the Access Control and Surveillance Solution at SACU. The proposal must clearly outline the planned implementation steps, from installation through to final commissioning.

9.2 The methodology should speak to how the bidder will approach the project, including preparation, installation and integration, system configuration, testing, training, documentation, and final handover. Proposals that are accompanied by

clear project plans detailing the sequencing of activities to be carried out and their planned implementation timelines will be viewed more favourably

10. DELIVERABLES AND PAYMENT MILESTONES

10.1 The project deliverables and associated payment schedule shall be as follows, with each payment released upon achievement of the corresponding milestone:

(a) **submission and approval of the Project Inception Report**, including the confirmed implementation schedule, the Secretariat shall release **ten percent (10%)** of the total project cost;

(b) **successful installation, configuration, and commissioning** of all access control and surveillance system component, along with completion of testing, user acceptance sign-off, and submission of the commissioning report, the Secretariat shall release **fifty percent (50%)** of the total project cost;

(c) **completion of end-user training, handover of system credentials, and delivery of final documentation** (system design, user manuals, configuration logs), the Secretariat shall release **thirty per cent (30%)** of the total project cost; and

(d) the expiry of the **30-day installation warranty period** without any unresolved defects or performance issues, the Secretariat shall release the remaining **ten per cent (10%)** of the total project cost.

11. EXPERTISE REQUIRED

11.1 The prospective bidders must possess the following experience:

(a) at least five (5) years' proven experience in the delivery and implementation of electronic Access Control and Surveillance Systems for medium-sized facilities (50+ users) and large facilities (100+ users); and

(b) successful delivery of a minimum of five (5) similar projects involving biometric access control, video surveillance, and integrated security management systems. Bidders must submit a portfolio of these completed projects, each with contactable client references.

11.2 The proposed implementation team must comprise professionals who:

(a) hold relevant professional certifications across the technologies included in the proposed solution. This may include, but is not limited to, electronic access control, IP surveillance systems, structured cabling, systems integration, and physical security technologies. Resumes and certificates for all key personnel must be included; and

(b) have demonstrable experience implementing integrated security solutions aligned with international security management practices or standards (e.g. ISO/IEC 27001, ISO/IEC 22301), regional safety frameworks, or national security compliance requirements where applicable.

12. SUBMISSION OF BIDS

12.1 All bidding proposals must be submitted electronically to: procurement@sacu.int.

12.2 All bidding proposals must be submitted electronically to: procurement@sacu.int. One (1) SET of the Technical and Financial proposal must be attached to the email submission in PDF format.

12.3 The deadline for submission of bids is 17h00 (Namibian time) on Friday, 31 October 2025.

13. The SACU Secretariat will set up a compulsory pre-bid meeting to be held at the SACU Secretariat (Julius K. Nyerere & Sir Seretse Khama Streets, Windhoek, Namibia) at 15h00 on Tuesday, 23 October 2025. This meeting will assist clarify the requirements for bid submission as well as to provide bidders with an opportunity of a guided tour to for viewing the current Access Control System and its components

14. EVALUATION OF BIDS & AWARD CRITERIA

14.1 ELIGIBILITY CRITERIA

(a) Only Bids received as specified in Section 12 (Submission of Bid Proposals) above will be considered.

(b) Bids will be disqualified if the following documents have not been submitted:

(i) a letter of introduction that identifies the bidder with a corporate letterhead. This Letter of Introduction (See Appendix B) should also contain:

i. a signature of the person(s) authorised to bind the organisation to statements made in the proposal;

ii. confirmation of the name of the bidder and acceptance by the bidder and any third parties of the conditions of the Request for Bid;

iii. written declaration that the bidder's current or past corporate or other interests does not give rise to a conflict of interest in connection with this Request for Bid;

iv. full Contact Details of any third-party involved in the proposal, if any; and

v. description of the role or element of proposal to be fulfilled by any third-party, if any;

(ii) a certified copy of a Certificate of Registration or Incorporation with the relevant national authorities for companies or close corporations;

(iii) proof of majority SACU citizen ownership that may be proven by any of the following methods:

i. a certified copy of each shareholding certificate currently in issue (the total shareholding certificates must aggregate 100% of all issued share capital); and proof of SACU citizenship by providing a certified copy of shareholders national identity card/document or valid passport; or

ii. a certified copy of the shareholder register issued by the duly appointed company secretary or external auditors; and proof of SACU citizenship by providing a certified copy of shareholders national identity card/document or valid passport; or

iii. an official letter from the external auditors or company secretary, describing the group structure and confirming that the ultimate holding company is majority (51%) owned by SACU citizens. This is only required where any shareholder is not a natural person.

(iv) a certified copy of a current (valid as at bid closing date) Good Standing Certificate or Tax Clearance Certificate from the relevant national authorities, or exemption thereof;

(v) a certified copy of the latest audited Annual Financial Statements in the case of private or public companies, or for close corporations the latest Annual Financial Statements. In either case, the reporting date is within 20 months from the Bid Closing Date. The audit report on the Annual Financial Statements should be issued by a member of the applicable regulatory authority in any SACU Member State and quote the membership number.

For close corporations, the latest Annual Financial Statements should be submitted prepared by a current member of the applicable regulatory authority in any SACU Member State;

(vi) a certified copy of a legal agreement for partnerships, consortiums and joint ventures, where applicable; and

(vii) in the case of partnerships, consortiums and joint ventures, all documents of each party in the arrangement and legal entities, must be submitted.

14.2 **AWARD CRITERIA**

(a) After the bidder has met the eligibility criteria, the technical evaluation is undertaken and awarded on the basis of the most economically advantageous proposal applying the following award criteria:

(i) **Technical Soundness of the proposed Access Control and Surveillance System:** assessment of the soundness of the bidder's proposal including its ability to meet or exceed the technical and operational requirements specified in Section 3 to Section 8 of this RFB;

(ii) **Methodology and Approach**: assessment of the soundness of the proposed methodology and implementation approach proposed by the bidder for delivering the products services described in Section 9 of this RFB. This will include the review of the bidder's proposed project plan and timelines, ensuring it aligns with the organisation's requirements and expectations for timely completion of the engagement;

(iii) **Bidding Company's Technical Expertise:** evaluation of the bidding company's technical expertise and knowledge in delivering Access Control and Surveillance Systems similar in scale and complexity to those described in Section 11 of this RFB. This must be substantiated through the company profile, a record of client engagements, and contactable references demonstrating successful past performance;

(iv) **Qualifications and Experience of Team Members:** evaluation of the bidder's technical resource persons' qualifications, certifications, and relevant experience in the implementation of Access Control and Surveillance Systems; and

(v) **Cost and Value for Money**: assessment of the bidder's pricing structure, considering the overall cost of the engagement and the value provided in terms of the quality of the provision of the services.

15. PRIME CONTRACTOR RELATIONSHIP

15.1 The SACU Secretariat will enter into a contract with only one successful bidder.

15.2 The selected bidder shall be solely responsible for the deliverables as specified in this document.

16. FINANCIAL ARRANGEMENT

16.1 Bidders are solely responsible for their own costs in preparing the Bid.

16.2 Payments for all services covered by this bid shall be made within 30 (thirty) days subject to receipt of appropriate invoices, the satisfactory completion of work, and adherence to the SACU Secretariat's Financial Policies and Guidelines.

16.3 SACU shall not be liable for any losses, damages, costs, charges or expenses caused by injuries to the bidder's personnel during the execution of their duties.

17. CONFIDENTIALITY

17.1 Bids submitted will not be revealed to any other bidders and will be treated as contractually binding.

17.2 The SACU Secretariat reserves the right to seek clarification or verification of any information in the Bids.

17.3 All information pertaining to the SACU Secretariat obtained by the bidder as a result of participation in this Request for Bid is confidential and must not be disclosed without written authorisation from the Executive Secretary of SACU.

17.4 The SACU Secretariat reserves the right to undertake a full background check on all references submitted prior to awarding the contract.

18. OWNERSHIP OF BIDS

18.1 All Bids, including supporting documents, submitted to the SACU Secretariat become the property of the SACU Secretariat.

18.2 Ownership of all data belonging to SACU whether under its control or the bidder's control shall continue to vest in SACU. Any data of whatever nature resulting from the provision of the Products and Services shall be the property of SACU and may be used by SACU without restriction. All data or information that may be shared with the successful bidder during the provision of the Products and Services shall upon termination of the contract, be returned to the SACU Secretariat.

19. MODIFICATION OF TERMS

19.1 The SACU Secretariat reserves the right to add, modify or omit certain portions of the Bids' scope at any time at its sole discretion. This includes the right to cancel this Request for Bid at any time prior to entering into a contract with the successful bidder.

20. CONTRACT ADMINISTRATION

20.1 The award will be subject to the successful conclusion of a Service Level Agreement (SLA) to confirm the Terms and Conditions of the proposal.

20.2 The SACU Secretariat reserves the right to negotiate the terms of the proposal and the value of any financial proposal submitted.

21. BID FORMAT

21.1 Bidders are requested to address the issues and requirements in the Document Checklist provided in Section 21 below and in Appendix A to ensure that their Bids receive full consideration.

22. DOCUMENTATION CHECKLIST

Have you submitted the following required information?	YES	NO
A Title (Cover) Page that outlines the Bid Number, Bid Description, Bid Closing Date, Bidding Organisation Name, Postal Address, Physical Address, Telephone No., Fax No., Mobile No., Email Address, Website and Full Names of two Contact Persons.		
A Letter of Introduction that meets the following criteria: i. identifies the bidder with a corporate letterhead, ii. is signed by the person(s) authorised to bind the organisation to statements made in the proposal; iii. contains a confirmation of acceptance by the bidder and any third parties of the conditions of the Request for Bid; iv. contains a written declaration that the bidder's current or past corporate or other interests does not give rise to a conflict of interest in connection with this Request for Bid; v. contains full contact details of any third-party involved in the proposal and a description of the role or element of proposal to be fulfilled by any third-party; and vi. contains a written confirmation that the Financial Proposal remains valid for 90 days.		
Profile of the bidder or consortium.		
Certified copy of the Certificate of Registration or Incorporation with the relevant national authorities.		
Certified copy of identity cards/documents or passports showing that the majority owner(s) or shareholders of the organisation or consortium are citizens of a SACU Member State. If the shareholder is not a natural person, then an official letter from the external auditors or company secretary confirming that the ultimate holding company is majority (<=51%) owned by SACU citizens.		
Certified copy of a current Good Standing Certificate or Tax Clearance Certificate from the relevant national authorities, or exemption thereof.		
A Certified Copy of the bidder's latest audited Annual Financial Statements in the case of private or public companies or the latest Annual Financial Statements for close corporations		

Have you submitted the following required information?	YES	NO
Certified copy of the latest audited Annual Financial Statements in the case of private or public companies, or for close corporations the latest Annual Financial Statements.		
Certified copy of a legal agreement for partnerships, consortiums and joint ventures, where applicable; and all documents of each party in the arrangement and legal entities, must be submitted.		
A detailed specification of the proposed Access Control and Surveillance Systems		
A detailed methodology that will be employed to implement the Implementation of Access Control and Surveillance System		
A Project Plan demonstrating how the bidder will complete the assignment		
A Project Plan demonstrating how the bidder will complete the assignment		
A schedule of five (5) or more similar assignments undertaken by the bidder		
A schedule of five (5) or more contactable references		
Proof of qualifications and experience of the team that will carry out the assignment		
The Financial Proposal is quoted in South African Rand (ZAR)		

Additional documents required from Consortiums or Partnerships	YES	NO
Written identification of the Primary Contracting Party		
Full details and eligibility criteria documents of all legal entities involved in the bid		
Certified copy of a legally binding partnership or consortium agreement		
Certified Proof that the majority owner(s) of the company or consortium are citizens of a SACU Member State (copy of ID's or Passports will suffice)		
Description of the role or element fulfilled by each legal entity		

APPENDIX A - FORMAT OF THE PROPOSAL

Bidders should address the issues and requirements in the sequence in which they appear in this Appendix.

1. General Information

(a) One page letter of introduction identifying the bidder and signed by the person(s) authorised to bind the organisation to statements made in the proposal.

(b) Title Page listing the Bid Number, Organisation Name, Postal Address, Physical Address, Telephone No., Fax No., Mobile No., Email Address, Website and Full Names of two Contact Persons.

(c) Profile of the Consultancy Firm or consortium.

(d) A record of previous similar assignments undertaken by the firm or consortium.

(e) Proof of qualifications and experience of the team that will deliver the goods or services, including the team leader.

(f) Full Contact Details of any third-parties involved in the proposal.

(g) Description of role or element of proposal to be fulfilled by any third-party.

(h) Confirmation of acceptance by the bidder and any third parties of the conditions of proposal.

(i) Declaration that bidder's current or past corporate or other interests does not give rise to a conflict of interest on this assignment.

(j) Certified copy of the Certificate of Registration or Incorporation with the relevant national authorities.

(k) Certified copy of identity cards/documents or passports showing that the majority owner(s) of the company or consortium are citizens of a SACU Member State. If the shareholder is not a natural person, then an official letter from the external auditors or company secretary confirming that the ultimate holding company is majority (51%) owned by SACU citizens.

(l) Certified copy of a current (valid as at bid closing date) Good Standing Certificate or Tax Clearance Certificate from the relevant national authorities, or exemption thereof.

(m) Where a consortium or a group of companies are jointly delivering a response, then the companies must:

(i) clearly state the name of the Primary Party with whom the SACU Secretariat will enter into an Agreement;

(ii) provide full details of each of the legal entities involved in the bid;

(iii) provide a certified copy of a legally binding partnership or consortium agreement; and

(iv) provide a detailed description of the role or element fulfilled by each legal entity involved in the bid.

2. Technical Proposal

2.1 A detailed technical proposal indicating a clear understanding of the specific requirements or scope of works, deliverables schedule and expertise, as per the Terms of Reference, should be submitted.

3. References

3.1 Bidders must provide a schedule of five (5) or more clients (contact names, physical addresses, and telephone numbers) who may be contacted for references in connection with the proposed assignment.

For example:

CLIENT	CONTACT NAME	TELEPHONE	PHYSICAL ADDRESS
ABC Corporation	Mr J. Doe	061-999 9999	20 ABC Street, Windhoek

3.2 Bidders must also provide a schedule of five (5) or more (recent and similar) assignments undertaken by the bidder. This schedule must indicate the client, the assignment that was undertaken, the year, the client's geographical location, and the financial value.

For example:

CLIENT	SERVICES PROVIDED	YEAR	LOCATION	FINANCIAL VALUE
ABC Corporation	Implementation of Access Control and Surveillance Systems	2011	Windhoek	R49,950

3.3 The SACU Secretariat reserves the right to undertake a full background check on all references submitted prior to awarding the contract.

4. Schedule of Costs/Financial Proposal

4.1 All costs must be quoted in South African Rands (ZAR). The schedule must take the following format:

(a) the total cost of the proposal (best and final offer);

(b) a full breakdown of the cost/price. This must clearly identify the once-off cost required for the setup and installation of the service and the ongoing costs for operating the environment;

(c) clearly identify the annual maintenance and support fees (as an optional extra) that should apply in the event that the Secretariat opts to subscribe for the service after the implementation of the system;

(d) an itemised breakdown of the cost of any options being proposed beyond that specified Request for Bid;

(e) the applicable rate of VAT in respect of each product and service being proposed;

(f) details of any other costs, taxes or duties which may be incurred; and

(g) confirmation that the Financial Proposal remains valid for 90 (ninety) days from the bid closing date.

5. Additional Information

5.1 Bidders may provide any other information which may be relevant to this proposal.

APPENDIX B – FORMAT OF THE LETTER OF INTRODUCTION

Private and confidential

REPLACEMENT OF THE ACCESS CONTROL AND SURVEILLANCE SYSTEM | BID NUMBER: SACU/0172026/PB

Name of Bidder (and Partner, if applicable) is pleased to submit this proposal. We believe we are uniquely equipped to assist the Southern African Customs Union (SACU) Secretariat with the provision of xxx.

Provide a brief motivation or summary of the assignment and the Bidder's skills, experience and track record.

Name of Bidder (and Partner, if applicable) hereby:

1. confirms acceptance of the terms and conditions of this Request for Bid; and
2. declares that our current or past corporate or other interests do not give rise to a conflict of interest on this assignment.

The contact details, role and any work to be undertaken by any third party involved in the proposal are as follows[1]:

1. xxx
2. xxx
3. xxx

I hereby declare that I am authorised to bind the organisation to statements made in this proposal.

Should you wish to discuss any aspect of this proposal or require any clarification, you are most welcome to contact me directly.

Yours sincerely,

(Name and Position)

[1] Delete this section if not applicable.