THE BORDER MANAGEMENT AUTHORITY (BMA) INVITES ALL INTERESTED PARTIES TO RESPOND TO THE REQUEST FOR PROPOSAL (RFP) FOR THE PROCUREMENT, INSTALLATION, CONFIGURATION, AND MANAGEMENT OF A SINGLE-VENDOR SECURE ACCESS SERVICE EDGE SOLUTION (SASE) FOR THREE (3) YEARS WITH PROFESSIONAL SERVICES.

The physical address for collection of Tender documents is:
Download from e-tender. SUBMISSION MUST BE THROUGH E-TENDER (e-submissions)

Queries relating to the issues of these documents may be addressed to suppliers.enquiries@bma.gov.za

The closing date **10 DECEMBER 2026** and closing time for Tenders is **11H00. BID DOCUMENTS ARE TO BE SUBMITTED THROUGH E-TENDER PORTAL (e-submission).** Telegraphic, telephonic, telex, facsimile, and late Tender Bids will not be accepted

BORDER MANAGEMENT AUTHORITY BID FORMS

ANNEXURE A	STANDARD BIDDING DOCUMENT
SECTION A	INVITATION TO BID
SECTION B	SBD 1 - TERMS AND CONDITIONS FOR BIDDING
SECTION C	SPECIAL INSTRUCTIONS REGARDING COMPLETION OF BID
SECTION D	REGISTRATION ON CENTRAL SUPPLIERS DATABASE
SECTION E	DECLARATION THAT INFORMATION ON CENTRAL SUPPLIER DATABASE IS CORRECT AND UP TO DATE
	AUTHORITY TO SIGN ON BEHALF OF THE COMPANY
SECTION F	PRICING SCHEDULE
SECTION G	DECLARATION OF INTEREST
SECTION H	PREFERENCE POINTS CLAIM FORM (SBD6.1)
SECTION I	CONTRACT FORM (SBD 7)
SECTION J	CONDITIONS OF BID
ANNEXURE B	GENERAL CONDITIONS OF CONTRACT (GCC)
SECTION K	OFFICIAL BRIEFING SESSION FORM
ANNEXURE C	SPECIFICATIONS / TERMS OF REFERENCE

SBD1
SECTION A
INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE BORDER MANAGEMENT ENTITY					
BID NUMBER:	**H004L2708RFP00137**	**CLOSING DATE:**	**10 DECEMBER 2026**	**CLOSING TIME:**	**11H00**
DESCRIPTION	**APPOINTMENT OF A SERVICE PROVIDER FOR THE PROCUREMENT, INSTALLATION, CONFIGURATION, AND MANAGEMENT OF A SINGLE-VENDOR SECURE ACCESS SERVICE EDGE SOLUTION (SASE) FOR A PERIOD OF THREE (3) YEARS.**				
BID DOCUMENTS ARE TO BE SUBMITTED THROUGH E-TENDER PORTAL (E-SUBMISSIONS)					
NON-COMPULSORY BRIEFING SESSION: 19 NOVEMBER 2026 ON MS TEAMS https://teams.microsoft.com/meet/3193862178849455?p=4ElHqM1Bclj9szqe09					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO			**TECHNICAL ENQUIRIES MAY BE DIRECTED TO:**		
CONTACT PERSON			**CONTACT PERSON**	**Khomotso Mokwele**	
TELEPHONE NUMBER			**TELEPHONE NUMBER**	**N/A**	
E-MAIL ADDRESS	suppliers.enquiries@bma.gov.za		**E-MAIL ADDRESS**	**ICTTechnicalEnquiries@bma.gov.za**	
SUPPLIER INFORMATION					
NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE UMBER	CODE		NUMBER		
CELLPHONE NUMBER					
FACSIMILE NUMBER	CODE		NUMBER		
E-MAIL ADDRESS					
VAT REGISTRATION NUMBER					
SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE SYSTEM PIN:		**OR** CENTRAL SUPPLIER DATABASE No:	MAAA	
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE	TICK APPLICABLE BOX] ☐ Yes ☐ No		B-BBEE STATUS LEVEL SWORN AFFIDAVIT	[TICK APPLICABLE BOX] ☐ Yes ☐ No	
[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/ SWORN AFFIDAVIT (FOR EMES & QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]					
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	☐Yes ☐No [IF YES ENCLOSE PROOF]		ARE YOU A FOREIGN BASED SUPPLIER FOR **THE GOODS /SERVICES /WORKS OFFERED?**	☐Yes ☐No [IF YES, ANSWER PART B:3]	

QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS

IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)?	☐ YES ☐ NO
DOES THE ENTITY HAVE A BRANCH IN THE RSA?	☐ YES ☐ NO
DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA?	☐ YES ☐ NO
DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA?	☐ YES ☐ NO
IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION?	☐ YES ☐ NO

IF THE ANSWER IS "NO" TO ALL OF THE ABOVE, THEN IT IS NOT A REQUIREMENT TO REGISTER FOR A TAX COMPLIANCE STATUS SYSTEM PIN CODE FROM THE SOUTH AFRICAN REVENUE SERVICE (SARS) AND IF NOT REGISTER AS PER 2.3 BELOW.

SECTION B
PART B
TERMS AND CONDITIONS FOR BIDDING

1.	**BID SUBMISSION:**
1.1.	BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.
1.2.	**ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED–(NOT TO BE RE-TYPED) OR IN THE MANNER PRESCRIBED IN THE BID DOCUMENT.**
1.3.	THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT, 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2017, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.
1.4.	**THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (SBD7).**
2.	**TAX COMPLIANCE REQUIREMENTS**
2.1	BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
2.2	BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS.
2.3	APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THE SARS WEBSITE WWW.SARS.GOV.ZA.
2.4	BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.
2.5	IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED; EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.
2.6	WHERE NO TCS IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.
2.7	NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE, COMPANIES WITH DIRECTORS WHO ARE PERSONS IN THE SERVICE OF THE STATE, OR CLOSE CORPORATIONS WITH MEMBERS PERSONS IN THE SERVICE OF THE STATE."

NB: FAILURE TO PROVIDE / OR COMPLY WITH ANY OF THE ABOVE PARTICULARS MAY RENDER THE BID INVALID.

SIGNATURE OF BIDDER: .....

CAPACITY UNDER WHICH THIS BID IS SIGNED: .....
(Proof of authority must be submitted e.g. company resolution)

DATE: .....

SECTION C

SPECIAL INSTRUCTIONS AND NOTICES TO BIDDERS REGARDING THE COMPLETION OF BIDDING FORMS

PLEASE NOTE THAT THIS CALL FOR BIDS IS SUBJECT TO TREASURY REGULATIONS 16A ISSUED IN TERMS OF THE PUBLIC FINANCE MANAGEMENT ACT, 1999.

1. Unless inconsistent with or expressly indicated otherwise by the context, the singular shall include the plural and vice versa and with words importing the masculine gender shall include the feminine and the neuter.
2. Under no circumstances whatsoever may the Bids forms be retyped or redrafted, but can be completed online without changing any words. Photocopies of the original Bids documentation may be used, but an original signature must appear on such photocopies.
3. The Respondent is advised to check the number of pages and to satisfy himself that none are missing or duplicated.
4. Bids submitted must be complete in all respects.
5. Bids shall be lodged at the address indicated not later than the closing time specified for their receipt, and in accordance with the directives in the Bids documents.
6. Each Bid shall be addressed in accordance with the directives in the bid documents and shall be lodged in a separate sealed envelope, with the name and address of the Respondent, the Bid number and closing date indicated on the envelope. The envelope shall not contain documents relating to any Bids other than that shown on the envelope. If this provision is not complied with, such Bids may be rejected as being invalid.
7. All Bids received in sealed envelopes with the relevant Bids numbers on the envelopes are kept unopened in safe custody until the closing time of the Bids. Where, however, a Bids is received open, it shall be sealed. If it is received without a Bids number on the envelope, it shall be opened, the Bid number ascertained, the envelope sealed, and the Bid number written on the envelope.
8. A specific box is provided for the receipt of Bids, and no Bids found in any other box or elsewhere subsequent to the closing date and time of Bids will be considered.
9. No Bids sent through the post/courier will be considered if it is received after the closing date and time stipulated in the BIDS documentation, and proof of posting/couriering will not be accepted as proof of delivery.
10. No Bids submitted by telefax, telegraphic will be considered.
11. Bids documents must not be included in packages containing samples. Such Bids may be rejected as being invalid.
12. Any alteration made by the Respondent must be initialed. If not initialed the Respondent may be disqualified.
13. Use of correcting fluid is prohibited
14. Bids will be opened in public as soon as practicable after the closing time of Bids.
15. Where practical, prices will be made public at the time of opening Bids.

Rights to Award

- Border Management Authority reserves the right to call for presentations from shortlisted suppliers or Reserves the Right to accept bids in Whole or In Part."
- Not to make any award in this bid or accept any proposals submitted,
- Award the project to more than one (1) Respondent for the same activity
- Request further technical/functional information from any Respondent after the closing date,
- Verify information and documentation of the Respondent(s),
- Not to accept any of the bid document submitted,
- To withdraw or amend any of the bid conditions by notice in writing to all Respondents prior to closing of the bid and post award, and
- If an incorrect award has been made to remedy the matter in any lawful manner it may deem fit.
- Apply objective criteria

- Service providers are not allowed to utilize employees that are non-South African Citizen, this may lead to contract termination unless vetted and having work permit.

Price Negotiation

BMA reserves the right to negotiate with the shortlisted Respondents prior and/or post award. The terms and conditions for negotiations will be communicated to the shortlisted Respondents prior to invitation to negotiations. The negotiation terms and conditions may include presentations and/or site visits. This phase is meant to ensure the conditions of bid and projects will be implementable for the achievement of the project objectives.

BMA supports the spirit of economic empowerment and recognizes that real empowerment can only be achieved through individuals and businesses conducting themselves in accordance with the Constitution and in an honest, fair, equitable, transparent and legally compliant manner. Against this background the BMA does not support any form of fronting.

Remuneration

•The service provider will be remunerated in South African Rands, on a fixed price (Inclusive of VAT) for the service rendered.

•Payment will be made within 30 days of receipt of the approved invoice according to an agreed payment schedule.

•Payment will be against the key deliverables as set out in section 4 above, provided professional-level quality standards have been met. Disputes as to what constitutes a reasonable standard will be referred to an agreed provider of arbitration services.

•Disbursements must not exceed 10% of the total amount paid to the service provider and will be paid only if original receipts are provided against a list of expenses that are agreed in advance of the costs being incurred.

THE EVALUATION WILL BE EVALUATED AS FOLLOWS:

Administrative Compliance		Mandatory Compliance
i.	SBD 1: Invitation bid (PART A)	REFER TO TOR PAGE 47 TO 48
ii.	Terms And Conditions for Bidding.	
iii.	Declaration of CSD Registration	
iv.	SBD3: Pricing Schedule	
v.	SBD 4 form: Bidders Disclosure	
vi.	SBD 6.1 form: Preference Points claim. Attach active BBBEE certificate or Affidavit	
vii.	SBD 7	

SECTION D

REGISTRATION ON THE CENTRAL SUPPLIERS DATABASE

1. In terms of the National Treasury Instruction Note, all suppliers of goods and services to the State are required to register on the Central Suppliers Database.

2. Prospective suppliers should self-register on the CSD website www.csd.gov.za

3. If a business is registered on the Database and it is found subsequently that false or incorrect information has been supplied, then the Entity may, without prejudice to any other legal rights or remedies it may have;

   3.1 cancel a bid or a contract awarded to such supplier, and the supplier would become liable for any damages if a less favourable bid is accepted or less favourable arrangements are made.

4. The same principles as set out in paragraph 3 above are applicable should the supplier fail to request updating of its information on the Central Suppliers Database, relating to changed particulars or circumstances.

5. IF THE SUPPLIER IS NOT REGISTERED AT THE CLOSING TIME OF BID, THE SUPPLIER WILL BE DISQUALIFIED AT THE BID EVALUATION PROCESS.

SECTION E
DECLARATION THAT INFORMATION ON CENTRAL SUPPLIER DATABASE IS CORRECT AND UP TO DATE
(To be completed by bidder)

THIS IS TO CERTIFY THAT I (name of bidder/authorized representative) ……

……....., WHO REPRESENTS (state name of bidder) ……...

…….....

CSD Registration Number.....

AM AWARE OF THE CONTENTS OF THE CENTRAL SUPPLIER DATABASE WITH RESPECT TO THE BIDDER'S DETAILS AND REGISTRATION INFORMATION, AND THAT THE SAID INFORMATION IS CORRECT AND UP TO DATE AS ON THE DATE OF SUBMITTING THIS BID.

AND I AM AWARE THAT INCORRECT OR OUTDATED INFORMATION MAY BE A CAUSE FOR DISQUALIFICATION OF THIS BID FROM THE BIDDING PROCESS, AND/OR POSSIBLE CANCELLATION OF THE CONTRACT THAT MAY BE AWARDED ON THE BASIS OF THIS BID.

.....
SIGNATURE OF BIDDER OR AUTHORISED REPRESENTATIVE

DATE: .....

Resolution to sign on behalf of Company (ensure all spaces highlighted are completed)

RESOLUTION of a meeting of the Board of "Directors / Members / Partners of:
.....
(legally correct full name and registration number, if applicable, of the Enterprise)
held at: ……..... (place) on…….....(date)

RESOLVED that:
The Enterprise submits a Tender to BMA in respect of the following:

Tender Reference Description:
…….....
(Project description as per Tender Document)

*Mr/Mrs/Ms ……..... in *his/her capacity as:
…….....(position)

And who will sign as follows: _____ (Signature)
and is hereby, authorised to sign the Tender and all other documents and/or correspondence in connection with and relating to this bid, as well as to sign any Contract, and any and all documentation, resulting from the award of any project to the Enterprise mentioned above.

No	NAME	CAPACITY	SIGNATURE
1			
2			
3			
4			
5			
6			
7			
8			

1. *Delete which is not applicable. 2. NB: This resolution must be signed by all the Directors / Members / Partners of the Tendering Enterprise. 3. Should the number of Directors /Members / Partners exceed the space available above, additional names and signatures must be supplied on a separate page

SECTION F
SBD 3.1
PRICING SCHEDULE – FIRM PRICES
(PURCHASES)

NOTE: **ONLY FIRM PRICES WILL BE ACCEPTED. NON-FIRM PRICES (INCLUDING PRICES SUBJECT TO RATES OF EXCHANGE VARIATIONS) WILL NOT BE CONSIDERED IN CASES WHERE DIFFERENT DELIVERY POINTS INFLUENCE THE PRICING, A SEPARATE PRICING SCHEDULE MUST BE SUBMITTED FOR EACH DELIVERY POINT**

Name of bidder…… Bid Number: H004L2708RFP00137
Closing Time: **11AM** Closing date: 10 DECEMBER 2026

Lead Time: ……**Days / Weeks**

Always submit your invoice to supplierinvoices@bma.gov.za

OFFER TO BE VALID FOR **120 DAYS** FROM THE CLOSING DATE OF BID.

ITEM NO.	Description	Frequency	Total price (excl vat)
1	PROCUREMENT, INSTALLATION, CONFIGURATION, AND MANAGEMENT OF A SINGLE-VENDOR SECURE ACCESS SERVICE EDGE SOLUTION (SASE) FOR THREE (3) YEARS WITH PROFESSIONAL SERVICES.	36 MONTHS	
Sub Total			
VAT AT 15%			
GRAND TOTAL (BID PRICE IN RSA CURRENCY WITH ALL APPLICABLE TAXES INCLUDED)			

The total cost amount must cover all costs associated with the service

I (full name)_____,in my capacity as_____, the duly authorized representative of_____(business name) hereby declares that the offer is in accordance with the attached specifications, notes to suppliers & accepts allconditions/clauses contained in the said documents.

Signature of the duly authorised representative		Date:

- Required by: ……
- At: ……

……

- Brand and model ……

- Country of origin ……

- Does the offer comply with the specification(s)? *YES/NO

- If not to specification, indicate deviation(s) ……

- Period required for delivery ……
*Delivery:

Firm/not firm

- Delivery basis ……

Note: All delivery costs must be included in the bid price, for delivery at the prescribed destination.

** “all applicable taxes” includes value- added tax, pay as you earn, income tax, unemployment insurance fund contributions and skills development levies.

*Delete if not applicable

SECTION G

SBD 4

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

Any person (natural or juristic) may make an offer or offers in terms of this invitation to bid. In line with the principles of transparency, accountability, impartiality, and ethics as enshrined in the Constitution of the Republic of South Africa and further expressed in various pieces of legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.

Where a person/s are listed in the Register for Tender Defaulters and / or the List of Restricted Suppliers, that person will automatically be disqualified from the bid process.

2. Bidder's declaration

2.1 Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest1 in the enterprise, employed by the state?

YES	
NO	

2.1.1 If so, furnish particulars of the names, individual identity numbers, and, if applicable, state employee numbers of sole proprietor/ directors / trustees / shareholders / members/ partners or any person having a controlling interest in the enterprise, in table below.

Full Name	Identity Number	Name of State institution

2.2 Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution?

YES	
NO	

2.2.1 If so, furnish particulars:

……

……

[1] the power, by one person or a group of persons holding the majority of the equity of an enterprise, alternatively, the person/s having the deciding vote or power to influence or to direct the course and decisions of the enterprise.

2.3 Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract?

YES	
NO	

2.3.1 If so, furnish particulars:
……
……

3 DECLARATION

I, the undersigned, (name)……. in submitting the accompanying bid, do hereby make the following statements that I certify to be true and complete in every respect:

3.1 I have read and I understand the contents of this disclosure;
3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;
3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium2 will not be construed as collusive bidding.
3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates.
3.4 The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.

3.5 There have been no consultations, communications, agreements or arrangements made by the bidder with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.

3.6 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and

[2] Joint venture or Consortium means an association of persons for the purpose of combining their expertise, property, capital, efforts, skill and knowledge in an activity for the execution of a contract.

or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT. I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTING AND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

…… ……
Signature Date

…… ……
Position Name of bidder

Every question must be answered individually on this form, whether a relationship is present or not: Failure to do so will invalidate your tender/bid

SECTION H
SBD 6.1

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2022

This preference form must form part of all tenders invited. It contains general information and serves as a claim form for preference points for specific goals.

NB: BEFORE COMPLETING THIS FORM, TENDERERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF THE TENDER AND PREFERENTIAL PROCUREMENT REGULATIONS, 2022

---

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to invitations to tender:

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2 **To be completed by the organ of state**

a) The applicable preference point system for this tender is the 80/20 preference point system.

b) Either the 90/10 or 80/20 preference point system will be applicable in this tender. The lowest/ highest acceptable tender will be used to determine the accurate system once tenders are received.

1.3 Points for this tender (even in the case of a tender for income-generating contracts) shall be awarded for:

(a) Price; and

(b) Specific Goals.

1.4 **To be completed by the organ of state:**

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	**80**
SPECIFIC GOALS	**20**
Total points for Price and SPECIFIC GOALS	**100**

1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.

1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

(a) **"tender"** means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;

(b) **"price"** means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;

(c) **"rand value"** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;

(d) **"tender for income-generating contracts"** means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and

(e) **"the Act"** means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3.1. POINTS AWARDED FOR PRICE

3.1.1 THE 80/20 OR 90/10 PREFERENCE POINT SYSTEMS

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20 **or** **90/10**

$$Ps = 80\left(1 - \frac{Pt - P\,min}{P\,min}\right) \text{ or } \quad Ps = 90\left(1 - \frac{Pt - P\,min}{P\,min}\right)$$

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmin = Price of lowest acceptable tender

3.2. FORMULAE FOR DISPOSAL OR LEASING OF STATE ASSETS AND INCOME GENERATING PROCUREMENT

3.2.1. POINTS AWARDED FOR PRICE

A maximum of 80 or 90 points is allocated for price on the following basis:

80/20 **or** **90/10**

$$Ps = 80\left(1 + \frac{Pt - P\,max}{P\,max}\right) \text{ or } \quad Ps = 90\left(1 + \frac{Pt - P\,max}{Pmax}\right)$$

Where

Ps = Points scored for price of tender under consideration

Pt = Price of tender under consideration

Pmax = Price of highest acceptable tender

4. POINTS AWARDED FOR SPECIFIC GOALS

4.1. In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:

4.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—

(a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or

(b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,

then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

Table 1: Specific goals for the tender and points claimed are indicated per the table below.
(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.
Note to tenderers: The tenderer must indicate how they claim points for each preference point system.)

The specific goals allocated points in terms of this tender	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points claimed (80/20 system) (To be completed by the tenderer)
The company is owned / director/s / shareholders by people who are Black. • 100% company owned by people who are Black = **10 points** • ≥51% and <100% company owned by people who are Black = **5 points** • >0% and <51% company owned by people who are Black = **2 points** • 0% of companies owned by people who are Black = **0 points**	10	
The company is owned / director/s / shareholders by people who are Women. • 100% company owned by people who are Women = **4 points** • ≥51% and <100% company owned by people who are Women = **2 points** • >0% and <51% company owned by people who are Women = **1 points** 0% company owned by people who are Women = **0 points**	4	
The company is owned / director/s / shareholders by people who are Youth. • 100% company owned by people who are Youth = **3 points** • ≥51% and <100% company owned by people who are Youth = **2 points** • >0% and <51% company owned by people who are Youth = **1 points** 0% company owned by people who are Youth = **0 points**	3	
The company is owned/director's/ shareholders by people who are Military Veterans. • 100% company owned by people who are Military Veterans = 3 **points** • ≥51% and <100% company owned by people who are Military Veterans = 2 **points** • >0% and <51% company owned by people who are Military Veterans = 1 **points** 0% company owned by people who are Military Veterans = **0 points**	3	

DECLARATION WITH REGARD TO COMPANY/FIRM

4.3. Name of company/firm……

4.4. Company registration number: ……

4.5. TYPE OF COMPANY/ FIRM

- □ Partnership/Joint Venture / Consortium
- □ One-person business/sole propriety
- □ Close corporation
- □ Public Company
- □ Personal Liability Company
- □ (Pty) Limited
- □ Non-Profit Company
- □ State Owned Company

[TICK APPLICABLE BOX]

4.6. I, the undersigned, who is duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the specific goals as advised in the tender, qualifies the company/ firm for the preference(s) shown and I acknowledge that:

i) The information furnished is true and correct;

ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;

iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 4.2, the contractor may be required to furnish documentary proof to the satisfaction of the organ of state that the claims are correct;

iv) If the specific goals have been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the organ of state may, in addition to any other remedy it may have –

(a) disqualify the person from the tendering process;
(b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
(c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
(d) recommend that the tenderer or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
(e) forward the matter for criminal prosecution, if deemed necessary.

……
SIGNATURE(S) OF TENDERER(S)

SURNAME AND NAME: ……
DATE: ……
ADDRESS: ……
……
……
……

SECTION I
SBD 7.1

CONTRACT FORM - PURCHASE OF GOODS/WORKS **(SIGN THIS PAGE AS THE SERVICE PROVIDER)**

THIS FORM MUST BE FILLED IN DUPLICATE BY BOTH THE SUCCESSFUL BIDDER (PART 1) AND THE PURCHASER (PART 2). BOTH FORMS MUST BE SIGNED IN THE ORIGINAL SO THAT THE SUCCESSFUL BIDDER AND THE PURCHASER WOULD BE IN POSSESSION OF ORIGINALLY SIGNED CONTRACTS FOR THEIR RESPECTIVE RECORDS.

PART 1 (TO BE FILLED IN BY THE BIDDER)

1. I hereby undertake to supply all or any of the goods and/or works described in the attached bidding documents to (name of institution) Border Management Authority in accordance with the requirements and specifications stipulated in bid number **H004L2708RFP00137** at the price/s quoted. My offer/s remain binding upon me and open for acceptance by the purchaser during the validity period indicated and calculated from the closing time of bid.
2. The following documents shall be deemed to form and be read and construed as part of this agreement:
   (i) Bidding documents, *viz*
   - Invitation to bid;
   - Tax clearance certificate;
   - Pricing schedule(s);
   - Authority to sign;
   - Preference claims for Broad Based Black Economic Empowerment Status Level of Contribution in terms of the Preferential Procurement Regulations 2011;
   - Declaration of interest;

   (ii) General Conditions of Contract; and
   (iii) Other (specify)
3. I confirm that I have satisfied myself as to the correctness and validity of my bid; that the price(s) and rate(s) quoted cover all the goods and/or works specified in the bidding documents; that the price(s) and rate(s) cover all my obligations and I accept that any mistakes regarding price(s) and rate(s) and calculations will be at my own risk.
4. I accept full responsibility for the proper execution and fulfilment of all obligations and conditions devolving on me under this agreement as the principal liable for the due fulfillment of this contract.
5. I declare that I have no participation in any collusive practices with any bidder or any other person regarding this or any other bid.
6. I confirm that I am duly authorised to sign this contract.

NAME (PRINT) ……
CAPACITY ……
SIGNATURE ……
NAME OF FIRM ……
DATE ……..

WITNESSES

1 ……..……

2. ……

SBD 7.1

CONTRACT FORM - PURCHASE OF GOODS/WORKS (IGNORE THIS PAGE AS THE SERVICE PROVIDER)

PART 2 (TO BE FILLED IN BY THE PURCHASER)

1. I _____ in my capacity as_____ accept your bid under reference number _____ dated _____for the supply of goods/works indicated hereunder and/or further specified in the annexure(s).

2. An official order indicating delivery instructions is forthcoming.

3. I undertake to make payment for the goods/works delivered in accordance with the terms and conditions of the contract, within 30 (thirty) days after receipt of an invoice accompanied by the delivery note.

ITEM NO.	PRICE (ALL APPLICABLE TAXES INCLUDED)	BRAND	DELIVERY PERIOD	B-BBEE STATUS LEVEL OF CONTRIBUTION	MINIMUM THRESHOLD FOR LOCAL PRODUCTION AND CONTENT (if applicable)

4. I confirm that I am duly authorised to sign this contract.

SIGNED AT ……ON……..

NAME (PRINT) …….

SIGNATURE …….

OFFICIAL STAMP

WITNESSES

1. ……

2. ……

SECTION J

CONDITIONS OF BID

1. I/We hereby bid to supply all or any of the supplies and/or to render all or any of the services described in the attached documents to the Border Management Authority on the terms and conditions and be in accordance with the specifications stipulated in the bid documents (and which shall be taken as part of and be incorporated into this bid) at the prices and on the terms regarding time for delivery and/or execution inserted therein.

2. I/we agree that:

   (a) the offer herein shall remain binding upon me and open for acceptance by the Entity during the validity period indicated and calculated from the closing time of the bid;
   (b) this bid and its acceptance shall be subject to Treasury Regulations 16A issued in terms of the Public Finance Management Act, 1999, the, with which I/we am fully acquainted;
   (c) if I/we withdraw my bid within the period for which I/we have agreed that the bid shall remain open for acceptance, or fail to fulfil the contract when called upon to do so, the Entity may, without prejudice to its other rights, agree to the withdrawal of my bid or cancel the contract that may have been entered into between me and the Entity. I/we will then pay to the Entity any additional expenses incurred by the Entity having either to accept any less favourable bid or, if fresh bids have to be invited, the additional expenditure incurred by the invitation of fresh bids and by the subsequent acceptance of any less favourable bid. The Entity shall have the right to recover such additional expenditure by set-off against monies which may be due to me under this or any other bid or contract or against any guarantee or deposit that may have been furnished by me or on my behalf for the due fulfillment of this or any other bid or contract and pending the ascertainment of the amount of such additional expenditure to retain such monies, guarantee or deposit as security for any loss the Entity may sustain by reason of my default;
   (d) if my bid is accepted, the acceptance may be communicated to me by registered post, and that the South African Post Office Limited shall be treated as delivery agent to me;
   (e) the law of the Republic of South Africa shall govern the contract created by the acceptance of my bid and I choose *domicilium citandi et executandi* in the Republic at (full physical address) :
   ….....

   ….....

3. I/we furthermore confirm that I/we have satisfied myself as to the correctness and validity of my bid: that the price(s), rate(s) and preference quoted cover all of the work/item(s) and my obligations under a resulting contract, and I accept that any mistakes regarding the price(s) and calculations will be at my risk.

4. I/we hereby accept full responsibility for the proper execution and fulfillment of all obligations and conditions devolving on me under this agreement, as the Principal(s) liable for the due fulfillment of this contract.

5. I/we agree that any action arising from this contract may in all respects be instituted against me and I/we hereby undertake to satisfy fully any sentence or judgment which may be pronounced against me as a result of such action.

6. I/we confirm that I/we have declared all and any interest that I or any persons related to my business has with regard to this bid or any related bids by completion of the Declaration of Interest Section.

7. CERTIFICATION OF CORRECTNESS OF INFORMATION SUPPLIED IN THIS DOCUMENT

I/we, THE UNDERSIGNED, WHO WARRANT THAT I AM DULY AUTHORISED TO DO SO ON BEHALF OF THE BIDDER, CERTIFY THAT THE INFORMATION SUPPLIED IN TERMS OF THIS DOCUMENT IS CORRECT AND TRUE, THAT THE SIGNATORY TO THIS DOCUMENT IS DULY AUTHORISED AND ACKNOWLEDGE THAT:

(1) The bidder will furnish documentary proof regarding any bidding issue to the satisfaction of the Entity, if requested to do so.

(2) If the information supplied is found to be incorrect and/or false then the Entity, in addition to any remedies it may have, may:-

(a) Recover from the contractor all costs, losses or damages incurred or sustained by the Entity as a result of the award of the contract, and/or

(b) Cancel the contract and claim any damages which the Entity may suffer by having to make less favourable arrangements after such cancellation.

SIGNED ON THIS …..... **DAY OF** …..... **20** …..... **AT** …….

…..... …..
SIGNATURE OF BIDDER OR DULY AUTHORISED REPRESENTATIVE **NAME IN BLOCK LETTERS**

ON BEHALF OF (BIDDER'S NAME) …..

CAPACITY OF SIGNATORY …..

NAME OF CONTACT PERSON (IN BLOCK LETTERS, PLEASE) ……..……

…….....

POSTAL ADDRESS ……..…….

…..

TELEPHONE NUMBER: ……..…….....

FAX NUMBER: ……..…….....

CELLULAR PHONE NUMBER: ……..…….....

E-MAIL ADDRESS: ……..…….....

ANNEXURE B: GENERAL CONDITIONS OF CONTRACT

1. Definitions

1. The following terms shall be interpreted as indicated:

1.1 “Closing time” means the date and hour specified in the bidding documents for the receipt of bids.

1.2 “Contract” means the written agreement entered into between the purchaser and the supplier, as recorded in the contract form signed by the parties, including all attachments and appendices thereto and all documents incorporated by reference therein.

1.3 “Contract price” means the price payable to the supplier under the contract for the full and proper performance of his contractual obligations.

1.4 “Corrupt practice” means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in contract execution.

1.5 "Countervailing duties" are imposed in cases where an enterprise abroad is subsidized by its government and encouraged to market its products internationally.

1.6 “Country of origin” means the place where the goods were mined, grown or produced or from which the services are supplied. Goods are produced when, through manufacturing, processing or substantial and major assembly of components, a commercially recognized new product results that is substantially different in basic characteristics or in purpose or utility from its components.

1.7 “Day” means calendar day.

1.8 “Delivery” means delivery in compliance of the conditions of the contract or order.

1.9 “Delivery ex stock” means immediate delivery directly from stock actually on hand.

1.10 “Delivery into consignees store or to his site” means delivered and unloaded in the specified store or depot or on the specified site in compliance with the conditions of the contract or order, the supplier bearing all risks and charges involved until the supplies are so delivered and a valid receipt is obtained.

1.11 "Dumping" occurs when a private enterprise abroad market its goods on own initiative in the RSA at lower prices than that of the country of origin and which have the potential to harm the local industries in the RSA.

1.12 ”Force majeure” means an event beyond the control of the supplier and not involving the supplier’s fault or negligence and not foreseeable. Such events may include, but is not restricted to, acts of the purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

1.13 “Fraudulent practice” means a misrepresentation of facts in order to influence a procurement process or the execution of a contract to the detriment of any bidder, and includes collusive practice among bidders (prior to or after bid submission) designed to establish bid prices at artificial non-competitive levels and to deprive the bidder of the benefits of free and open competition.

1.14 “GCC” means the General Conditions of Contract.

1.15 “Goods” means all of the equipment, machinery, and/or other materials that the supplier is required to supply to the purchaser under the contract.

1.16 “Imported content” means that portion of the bidding price represented by the cost of components, parts or materials which have been or are still to be imported (whether by the supplier or his subcontractors) and which costs are inclusive of the costs abroad, plus freight and other direct importation costs such as landing costs, dock dues, import duty, sales duty or other similar tax or duty at the South African place of entry as well as transportation and handling charges to the factory in the Republic where the supplies covered by the bid will be manufactured.

1.17 “Local content” means that portion of the bidding price which is not included in the imported content provided that local manufacture does take place.

1.18 "Manufacture" means the production of products in a factory using labour, materials, components and machinery and includes other related value-adding activities.

1.19 "Order" means an official written order issued for the supply of goods or works or the rendering of a service.

1.20 "Project site," where applicable, means the place indicated in bidding documents.

1.21 "Purchaser" means the organization purchasing the goods.

1.22 "Republic" means the Republic of South Africa.

1.23 "SCC" means the Special Conditions of Contract.

1.24 "Services" means those functional services ancillary to the supply of the goods, such as transportation and any other incidental services, such as installation, commissioning, provision of technical assistance, training, catering, gardening, security, maintenance and other such obligations of the supplier covered under the contract.

1.25 "Written" or "in writing" means handwritten in ink or any form of electronic or mechanical writing.

2. Application

2.1 These general conditions are applicable to all bids, contracts and orders including bids for functional and professional services, sales, hiring, letting and the granting or acquiring of rights, but excluding immovable property, unless otherwise indicated in the bidding documents.

2.2 Where applicable, special conditions of contract are also laid down to cover specific supplies, services or works.

2.3 Where such special conditions of contract are in conflict with these general conditions, the special conditions shall apply.

3. General

3.1 Unless otherwise indicated in the bidding documents, the purchaser shall not be liable for any expense incurred in the preparation and submission of a bid. Where applicable a non-refundable fee for documents may be charged.

3.2 With certain exceptions, invitations to bid are only published in the Government Tender Bulletin. The Government Tender Bulletin may be obtained directly from the Government Printer, Private Bag X85, Pretoria 0001, or accessed electronically from www.treasury.gov.za

4. Standards

4.1 The goods supplied shall conform to the standards mentioned in the bidding documents and specifications.

5. Use of contract documents and information; inspection.

5.1 The supplier shall not, without the purchaser's prior written consent, disclose the contract, or any provision thereof, or any specification, plan, drawing, pattern, sample, or information furnished by or on behalf of the purchaser in connection therewith, to any person other than a person employed by the supplier in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only so far as may be necessary for purposes of such performance.

5.2 The supplier shall not, without the purchaser's prior written consent, make use of any document or information mentioned in GCC clause 5.1 except for purposes of performing the contract.

5.3 Any document, other than the contract itself mentioned in GCC clause 5.1 shall remain the property of the purchaser and shall be returned (all copies) to the purchaser on completion of the supplier's performance under

the contract if so required by the purchaser.

5.4 The supplier shall permit the purchaser to inspect the supplier's records relating to the performance of the supplier and to have them audited by auditors appointed by the purchaser, if so required by the purchaser.

6. Patent rights

6.1 The supplier shall indemnify the purchaser against all third-party claims of infringement of patent, trademark, or industrial design rights arising from use of the goods or any part thereof by the purchaser.

7. Performance security

7.1 Within thirty (30) days of receipt of the notification of contract award, the successful bidder shall furnish to the purchaser the performance security of the amount specified in SCC.

7.2 The proceeds of the performance security shall be payable to the purchaser as compensation for any loss resulting from the supplier's failure to complete his obligations under the contract.

7.3 The performance security shall be denominated in the currency of the contract or in a freely convertible currency acceptable to the purchaser and shall be in one of the following forms:

(a) a bank guarantee or an irrevocable letter of credit issued by a reputable bank located in the purchaser's country or abroad, acceptable to the purchaser, in the form provided in the bidding documents or another form acceptable to the purchaser; or

(b) a cashier's or certified cheque

7.4 The performance security will be discharged by the purchaser and returned to the supplier not later than thirty (30) days following the date of completion of the supplier's performance obligations under the contract, including any warranty obligations, unless otherwise specified in SCC.

8. Inspections, tests and analyses

8.1 All pre-bidding testing will be for the account of the bidder.

8.2 If it is a bid condition that supplies to be produced or services to be rendered should at any stage during production or execution or on completion be subject to inspection, the premises of the bidder or contractor shall be open, at all reasonable hours, for inspection by a representative of the Entity or an organization acting on behalf of the Entity.

8.3 If there are no inspection requirements indicated in the bidding documents and no mention is made in the contract, but during the contract period it is decided that inspections shall be carried out, the purchaser shall itself make the necessary arrangements, including payment arrangements with the testing authority concerned.

8.4 If the inspections, tests and analyses referred to in clauses 8.2 and 8.3 show the supplies to be in accordance with the contract requirements, the cost of the inspections, tests and analyses shall be defrayed by the purchaser.

8.5 Where the supplies or services referred to in clauses 8.2 and 8.3 do not comply with the contract requirements, irrespective of whether such supplies or services are accepted or not, the cost in connection with these inspections, tests or analyses shall be defrayed by the supplier.

8.6 Supplies and services which are referred to in clauses 8.2 and 8.3 and which do not comply with the contract requirements may be rejected.

8.7 Any contract supplies may on or after delivery be inspected, tested or analyzed and may be rejected if found not to comply with the requirements of the contract. Such rejected supplies shall be held at the cost and risk of the supplier who shall, when called upon, remove them immediately at his own cost and forthwith substitute them with supplies which do comply with the requirements of the contract. Failing such removal the rejected supplies shall be returned at the suppliers cost and risk. Should the supplier fail to provide the substitute

supplies forthwith, the purchaser may, without giving the supplier further opportunity to substitute the rejected supplies, purchase such supplies as may be necessary at the expense of the supplier.

8.8 The provisions of clauses 8.4 to 8.7 shall not prejudice the right of the purchaser to cancel the contract on account of a breach of the conditions thereof, or to act in terms of Clause 23 of GCC.

9. Packing

9.1 The supplier shall provide such packing of the goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the contract. The packing shall be sufficient to withstand, without limitation, rough handling during transit and exposure to extreme temperatures, salt and precipitation during transit, and open storage. Packing, case size and weights shall take into consideration, where appropriate, the remoteness of the goods' final destination and the absence of heavy handling facilities at all points in transit.

9.2 The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the contract, including additional requirements, if any, specified in SCC, and in any subsequent instructions ordered by the purchaser.

10. Delivery and documents

10.1 Delivery of the goods shall be made by the supplier in accordance with the terms specified in the contract. The details of shipping and/or other documents to be furnished by the supplier are specified in SCC.

10.2 Documents to be submitted by the supplier are specified in SCC.

11. Insurance

11.1 The goods supplied under the contract shall be fully insured in a freely convertible currency against loss or damage incidental to manufacture or acquisition, transportation, storage and delivery in the manner specified in the SCC.

12. Transportation

12.1 Should a price other than an all-inclusive delivered price be required, this shall be specified in the SCC.

13. Incidental Services

13.1 The supplier may be required to provide any or all of the following services, including additional services, if any, specified in SCC:

(a) performance or supervision of on-site assembly and/or commissioning of the supplied goods;
(b) furnishing of tools required for assembly and/or maintenance of the supplied goods;
(c) furnishing of a detailed operations and maintenance manual for each appropriate unit of the supplied goods;
(d) performance or supervision or maintenance and/or repair of the supplied goods, for a period of time agreed by the parties, provided that this service shall not relieve the supplier of any warranty obligations under this contract; and
(e) training of the purchaser's personnel, at the supplier's plant and/or on-site, in assembly, start-up, operation, maintenance, and/or repair of the supplied goods.

13.2 Prices charged by the supplier for incidental services, if not included in the contract price for the goods, shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the supplier for similar services.

14. Spare parts

14.1 As specified in SCC, the supplier may be required to provide any or all of the following materials, notifications, and information pertaining to spare parts manufactured or distributed by the supplier:

(a) such spare parts as the purchaser may elect to purchase from the supplier, provided that this election shall not relieve the supplier of any warranty obligations under the contract; and

(b) in the event of termination of production of the spare parts:
  (i) Advance notification to the purchaser of the pending termination, in sufficient time to permit the purchaser to procure needed requirements; and
  (ii) following such termination, furnishing at no cost to the purchaser, the blueprints, drawings, and specifications of the spare parts, if requested.

15. Warranty

15.1 The supplier warrants that the goods supplied under the contract are new, unused, of the most recent or current models, and that they incorporate all recent improvements in design and materials unless provided otherwise in the contract. The supplier further warrants that all goods supplied under this contract shall have no defect, arising from design, materials, or workmanship (except when the design and/or material is required by the purchaser's specifications) or from any act or omission of the supplier, that may develop under normal use of the supplied goods in the conditions prevailing in the country of final destination.

15.2 This warranty shall remain valid for twelve (12) months after the goods, or any portion thereof as the case may be, have been delivered to and accepted at the final destination indicated in the contract, or for eighteen (18) months after the date of shipment from the port or place of loading in the source country, whichever period concludes earlier, unless specified otherwise in SCC.

15.3 The purchaser shall promptly notify the supplier in writing of any claims arising under this warranty.

15.4 Upon receipt of such notice, the supplier shall, within the period specified in SCC and with all reasonable speed, repair or replace the defective goods or parts thereof, without costs to the purchaser.

15.5 If the supplier, having been notified, fails to remedy the defect(s) within the period specified in SCC, the purchaser may proceed to take such remedial action as may be necessary, at the supplier's risk and expense and without prejudice to any other rights which the purchaser may have against the supplier under the contract.

16. Payment

16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in SCC.

16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfillment of other obligations stipulated in the contract.

16.3 Payments shall be made promptly by the purchaser, but in no case later than thirty (30) days after submission of an invoice or claim by the supplier.

16.4 Payment will be made in Rand unless otherwise stipulated in SCC.

17. Prices

17.1 Prices charged by the supplier for goods delivered and services performed under the contract shall not vary from the prices quoted by the supplier in his bid, with the exception of any price adjustments authorized in SCC or in the purchaser's request for bid validity extension, as the case may be.

18. Contract amendments

18.1 No variation in or modification of the terms of the contract shall be made except by written amendment signed by the parties concerned.

19. Assignment

19.1 The supplier shall not assign, in whole or in part, its obligations to perform under the contract, except with the purchaser's prior written consent.

20. Subcontracts

20.1 The supplier shall notify the purchaser in writing of all subcontracts awarded under this contracts if not already specified in the bid. Such notification, in the original bid or later, shall not relieve the supplier from any liability or obligation under the contract.

21. Delays in the supplier's performance

21.1 Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.

21.2 If at any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.

21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national entity, Provincial entity, or a local authority.

21.4 The right is reserved to procure outside of the contract small quantities or to have minor essential services executed if an emergency arises, the supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily available.

21.5 Except as provided under GCC Clause 25, a delay by the supplier in the performance of its delivery obligations shall render the supplier liable to the imposition of penalties, pursuant to GCC Clause 22, unless an extension of time is agreed upon pursuant to GCC Clause 21.2 without the application of penalties.

21.6 Upon any delay beyond the delivery period in the case of a supplies contract, the purchaser shall, without cancelling the contract, be entitled to purchase supplies of a similar quality and up to the same quantity in substitution of the goods not supplied in conformity with the contract and to return any goods delivered later at the supplier's expense and risk, or to cancel the contract and buy such goods as may be required to complete the contract and without prejudice to his other rights, be entitled to claim damages from the supplier.

22. Penalties

22.1 Subject to GCC Clause 25, if the supplier fails to deliver any or all of the goods or to perform the services within the period(s) specified in the contract, the purchaser shall, without prejudice to its other remedies under the contract, deduct from the contract price, as a penalty, a sum calculated on the delivered price of the delayed goods or unperformed services using the current prime interest rate calculated for each day of the delay until actual delivery or performance. The purchaser may also consider termination of the contract pursuant to GCC Clause 23.

23. Termination for default

23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:
(a) if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;
(b) if the Supplier fails to perform any other obligation(s) under the contract; or
(c) if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

23.2 In the event the purchaser terminates the contract in whole or in part, the purchaser may procure, upon such terms and in such manner as it deems appropriate, goods, works or services similar to those undelivered, and the supplier shall be liable to the purchaser for any excess costs for such similar goods, works or services. However, the supplier shall continue performance of the contract to the extent not terminated.

23.3 Where the purchaser terminates the contract in whole or in part, the purchaser may decide to impose a restriction penalty on the supplier by prohibiting such supplier from doing business with the public sector for a period not exceeding 10 years.

23.4 If a purchaser intends imposing a restriction on a supplier or any person associated with the supplier, the supplier will be allowed a time period of not more than fourteen (14) days to provide reasons why the envisaged restriction should not be imposed. Should the supplier fail to respond within the stipulated fourteen (14) days

the purchaser may regard the intended penalty as not objected against and may impose it on the supplier.

23.5 Any restriction imposed on any person by the Accounting Officer / Authority will, at the discretion of the Accounting Officer / Authority, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which enterprise or person the first-mentioned person, is or was in the opinion of the Accounting Officer / Authority actively associated.

23.6 If a restriction is imposed, the purchaser must, within five (5) working days of such imposition, furnish the National Treasury, with the following information:
(i) the name and address of the supplier and / or person restricted by the purchaser;
(ii) the date of commencement of the restriction
(iii) the period of restriction; and
(iv) the reasons for the restriction.

These details will be loaded in the National Treasury's central database of suppliers or persons prohibited from doing business with the public sector.

23.7 If a court of law convicts a person of an offence as contemplated in sections 12 or 13 of the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004, the court may also rule that such person's name be endorsed on the Register for Tender Defaulters. When a person's name has been endorsed on the Register, the person will be prohibited from doing business with the public sector for a period not less than five years and not more than 10 years. The National Treasury is empowered to determine the period of restriction and each case will be dealt with on its own merits. According to section 32 of the Act the Register must be open to the public. The Register can be perused on the National Treasury website.

24. Anti-dumping and countervailing duties and rights

24.1 When, after the date of bid, provisional payments are required, or antidumping or countervailing duties are imposed, or the amount of a provisional payment or anti-dumping or countervailing right is increased in respect of any dumped or subsidized import, the State is not liable for any amount so required or imposed, or for the amount of any such increase. When, after the said date, such a provisional payment is no longer required or any such anti-dumping or countervailing right is abolished, or where the amount of such provisional payment or any such right is reduced, any such favourable difference shall on demand be paid forthwith by the contractor to the State or the State may deduct such amounts from moneys (if any) which may otherwise be due to the contractor in regard to supplies or services which he delivered or rendered, or is to deliver or render in terms of the contract or any other contract or any other amount which may be due to him.

25. Force Majeure

25.1 Notwithstanding the provisions of GCC Clauses 22 and 23, the supplier shall not be liable for forfeiture of its performance security, damages, or termination for default if and to the extent that his delay in performance or other failure to perform his obligations under the contract is the result of an event of force majeure.

25.2 If a force majeure situation arises, the supplier shall promptly notify the purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the purchaser in writing, the supplier shall continue to perform its obligations under the contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the force majeure event.

26. Termination for insolvency

26.1 The purchaser may at any time terminate the contract by giving written notice to the supplier if the supplier becomes bankrupt or otherwise insolvent. In this event, termination will be without compensation to the supplier, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the purchaser.

27. Settlement of Disputes

27.1 If any dispute or difference of any kind whatsoever arises between the purchaser and the supplier in connection

with or arising out of the contract, the parties shall make every effort to resolve amicably such dispute or difference by mutual consultation.

27.2 If, after thirty (30) days, the parties have failed to resolve their dispute or difference by such mutual consultation, then either the purchaser or the supplier may give notice to the other party of his intention to commence with mediation. No mediation in respect of this matter may be commenced unless such notice is given to the other party.

27.3 Should it not be possible to settle a dispute by means of mediation, it may be settled in a South African court of law.

27.4 Mediation proceedings shall be conducted in accordance with the rules of procedure specified in the SCC.

27.5 Notwithstanding any reference to mediation and/or court proceedings herein,
(a) the parties shall continue to perform their respective obligations under the contract unless they otherwise agree; and
(b) the purchaser shall pay the supplier any monies due the supplier.

28. Limitation of liability

28.1 Except in cases of criminal negligence or willful misconduct, and in the case of infringement pursuant to Clause 6;
(a) the supplier shall not be liable to the purchaser, whether in contract, tort, or otherwise, for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier to pay penalties and/or damages to the purchaser; and
(b) the aggregate liability of the supplier to the purchaser, whether under the contract, in tort or otherwise, shall not exceed the total contract price, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment.

29. Governing language

29.1 The contract shall be written in English. All correspondence and other documents pertaining to the contract that is exchanged by the parties shall also be written in English.

30. Applicable law

30.1 The contract shall be interpreted in accordance with South African laws, unless otherwise specified in SCC.

31. Notices

31.1 Every written acceptance of a bid shall be posted to the supplier concerned by registered or certified mail and any other notice to him shall be posted by ordinary mail to the address furnished in his bid or to the address notified later by him in writing and such posting shall be deemed to be proper service of such notice

31.2 The time mentioned in the contract documents for performing any act after such aforesaid notice has been given, shall be reckoned from the date of posting of such notice.

32. Taxes and duties

32.1 A foreign supplier shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the purchaser's country.

32.2 A local supplier shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted goods to the purchaser.

32.3 No contract shall be concluded with any bidder whose tax matters are not in order. Prior to the award of a bid the Entity must be in possession of a tax clearance certificate, submitted by the bidder. This certificate must be an original issued by the South African Revenue Services.

33. National Industrial Participation (NIP) Programme

33.1 The NIP Programme administered by the Entity of Trade and Industry shall be applicable to all contracts that are subject to the NIP obligation.

34 Prohibition of Restrictive practices

34.1 In terms of section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, an agreement between, or concerted practice by, firms, or a decision by an association of firms, is prohibited if it is between parties in a horizontal relationship and if a bidder (s) is / are or a contractor(s) was / were involved in collusive bidding (or bid rigging).

34.2 If a bidder(s) or contractor(s), based on reasonable grounds or evidence obtained by the purchaser, has / have engaged in the restrictive practice referred to above, the purchaser may refer the matter to the Competition Commission for investigation and possible imposition of administrative penalties as contemplated in the Competition Act No. 89 of 1998.

SECTION K

OFFICIAL BRIEFING SESSION/SITE INSPECTION CERTIFICATE: APPLICABLE IF ITS COMPLUSORY PHYSICAL BREIFING

N.B.: this form is only to be included and completed when applicable to the bid.

Site/building/institution involved: border management entity

Bid no: H004L2708RFP00137

SERVICE: THE BORDER MANAGEMENT AUTHORITY (BMA) INVITES ALL INTERESTED PARTIES TO RESPOND TO THE REQUEST FOR PROPOSAL (RFP) FOR THE PROCUREMENT, INSTALLATION, CONFIGURATION, AND MANAGEMENT OF A SINGLE-VENDOR SECURE ACCESS SERVICE EDGE SOLUTION (SASE) FOR THREE (3) YEARS WITH PROFESSIONAL SERVICES.

****

This is to certify that (name) .....

On behalf of .....

Visited and inspected the site on .....(date)

And is therefore familiar with the circumstances and the scope of the service to be rendered.

.....
Signature of Bidder or Authorised Representative
(Print Name)

Date: .....

.....
signature of entity representative
(print name)

entity stamp

ANNEXURE E

TERMS OF REFERENCE

THE BORDER MANAGEMENT AUTHORITY (BMA) INVITES ALL INTERESTED PARTIES TO RESPOND TO THE REQUEST FOR PROPOSAL (RFP) FOR THE PROCUREMENT, INSTALLATION, CONFIGURATION, AND MANAGEMENT OF A SINGLE-VENDOR SECURE ACCESS SERVICE EDGE SOLUTION (SASE) FOR THREE (3) YEARS WITH PROFESSIONAL SERVICES.

1. INTRODUCTION

1.1. Purpose

These Terms of Reference (ToR) aim to procure and implement a Secure Access Service Edge (SASE) solution that meets the Border Management Authority's (BMA) evolving security needs in a hybrid, cloud-first environment. As traditional perimeter-based security models no longer suffice, the SASE solution is designed to provide secure, policy-driven access to the internet, cloud services, and internal applications, regardless of user location, while ensuring compliance with data protection and data residency requirements, providing transparency of data processing and storage locations, enhancing threat protection, and improving the user experience through a unified, cloud-delivered security architecture.

1.2. Background

1.2.1. The BMA

The Border Management Authority (BMA) is a national government entity mandated to manage and secure South Africa’s borders in an integrated, efficient, and coordinated manner. The BMA plays a central role in facilitating legitimate trade and travel, preventing illegal cross-border activities, and ensuring the integrity of the country’s ports of entry and border law enforcement operations.

1.2.2. Operational Landscape and Current IT environment context and challenges

a) The BMA operates in a highly sensitive, distributed, and geographically dispersed technology environment comprising Ports of Entry, remote and mobile users, cloud-hosted systems and services, and planned future on-premises infrastructure. This operating model requires a modern security architecture that consistently protects users, applications, data, and services regardless of location or hosting environment.

b) The current security architecture presents several challenges in supporting this distributed environment. These include private organisational applications that are accessible over the public internet, decentralised security visibility and policy enforcement, and inadequate network security capabilities, including firewalling, intrusion detection and prevention, and centralised security monitoring and traffic inspection. These limitations increase exposure to cyber threats and make it difficult to consistently enforce security controls across users, applications, cloud environments, and locations.

c) Therefore, the BMA requires a future-ready Secure Access Service Edge (SASE) solution that provides secure, identity- and context-aware access to private applications, internet services, Software-as-a-Service (SaaS), and other organisational resources. The solution must provide centralised policy

management, visibility, monitoring, and reporting via a unified management platform, while enabling security inspection and policy enforcement through cloud-delivered Points of Presence (PoPs). Internet traffic should not be required to backhaul to a central BMA site for security inspection.

d) The proposed solution must provide integrated security capabilities including, among others, Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), Firewall-as-a-Service (FWaaS), DNS Security, TLS inspection/decryption, Threat Prevention, intrusion prevention, and URL filtering. The solution must support secure access across internet, SaaS, cloud-hosted, remote, and future on-premises environments and integrate with the BMA's existing identity and security ecosystem

e) The implementation of the solution will enable the BMA to reduce unnecessary public exposure of private applications, strengthen access controls and threat protection, improve security visibility and policy enforcement, and establish a scalable security architecture capable of supporting the BMA's evolving hybrid technology environment

2. AIM AND OBJECTIVES

This procurement aims to appoint a qualified, experienced, and suitable service provider to supply, implement, configure, support, and maintain a SASE solution for three (3) years.

a) Implement a scalable, secure, and cloud-delivered SASE solution capable of supporting distributed operations, remote access, and hybrid environments.
b) Ensure the protection, confidentiality, integrity, and appropriate governance and compliance of organisational and personal information in line with applicable legislation, regulations, policies, and standards,
c) Enable secure access to cloud services, internet, on-premises, and private applications through unified security controls
d) Enforce Zero Trust access principles and identity-driven security controls

3. SCOPE OF WORK

The appointed service provider must supply, implement, configure, support, and maintain a single-vendor Secure Access Service Edge (SASE) solution.

3.1. High-level Implementation and Configuration Services

a) Deploy and configure a Secure Access Service Edge (SASE) platform with capabilities including, among others, Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), Firewall-as-a-Service for all ports and protocols (FWaaS), threat prevention, TLS decryption, URL filtering, DNS security, inline sandboxing, Secure Enterprise Browser, and Dedicated Egress IP.
b) Configure security policies, access controls, inspection policies, and traffic routing in line with BMA security requirements and best practices, including independence of a PAC file for traffic forwarding.
c) Implement secure web access and secure private application connectivity for authorised users.

3.2. Technical and functional SASE Solution Specifications/Requirements

The following requirements guide bidders in proposing a Secure Access Service Edge (SASE) solution aligned with the BMA's strategic growth objectives, digital transformation initiatives, cybersecurity strategy, operational requirements, and cost-optimisation objectives.

3.2.1. Architecture

a) The solution must provide consistent networking and security controls for access to the corporate data centre, public cloud, SaaS, and the internet.
b) The solution must be capable of managing traffic distribution between the different network links on a site.
c) The proposed solution shall operate an isolated data plane, with dedicated compute and IP address resources, to ensure enhanced security and resource isolation.
d) The proposed solution must offer multi-tenancy, which can create different instances for different business units if needed.
e) The solution must support streaming media and online meeting applications without requiring split tunnelling, while maintaining acceptable performance and enforcing the BMA security policies.
f) The solution shall provide access to sites hosting servers accessed by clients everywhere. Overlay topology shall allow direct communication between these sites without transiting through a hub.
g) The solution must support micro-segmented access to applications using Layer 3-7 policies defined on a per-user / group level, reducing the impact of a compromise (if any).
h) The bidder must present a detailed backbone network map identifying the main international backbone links and all the POPs.
i) The Solution should not backhaul traffic for inspection to a central site and should not depend on PAC files for traffic forwarding
j) The BMA wants a solution that provides a set of in-country public IP addresses.
k) The solution does not rely on split-tunnel for streaming media and/or online meeting solutions.
l) The solution must support all leading Operating Systems, including Windows, macOS, Apple iOS, and Android.

3.2.2. Core Security Components Requirements

a) **Secure Web Gateway -** Enforce organisational security policies and inspect internet and web traffic to protect users against web-based threats.
b) **URL filtering -** Control access to websites and web applications based on URL categories, risk, reputation and organisational security policies.
c) **Zero Trust Network Access (ZTNA) -** Provide identity- and context-aware, least-privilege access to authorised private applications and resources without exposing users to the underlying network. The solution should support continuous assessment of user, device and application context.

d) **TLS Decryption/Inspection -** Support inspection of encrypted TLS traffic to identify malicious activity, threats and policy violations, subject to configurable decryption policies and exclusions. Must support TLS 1.3, and whether it allows decryption based on user/user group/ and source/destination IP and Port

e) **Firewall-as-a-Service (FWaaS) -** Provide cloud-delivered next-generation firewall capabilities, including application-aware (Layer 7) inspection, identity-aware security policy enforcement, application control and threat prevention for all ports and protocols

f) **Threat Prevention/IPS/Anti-malware/Antivirus -** Provide integrated threat prevention capabilities, including intrusion prevention, anti-malware, behavioural and signature-based detection, command-and-control (C2) detection and blocking, and protection against known and unknown threats.

g) **DNS Security -** Detect and prevent DNS-based threats, including access to malicious domains, command-and-control infrastructure and other malicious DNS activity.

h) **Cloud-Based Sandboxing –** Provide cloud-based inline sandboxing and advanced malware analysis to detect and prevent unknown and zero-day threats without requiring traffic to be backhauled to a BMA central site for analysis

i) **Dedicated Egress IP –** Provide dedicated/static public egress IP address(es) to support IP allowlisting, application access policies and integration with external services requiring known source IP addresses.

j) **Secure Enterprise Browser –** Provide a secure enterprise browser capability for managed and unmanaged devices, supporting secure access to SaaS and private web applications, granular data and session controls, and protection against browser-based threats. The capability should support deployment independently of the endpoint SASE agent where required

3.2.3. Core functional Security Requirements.

a) The solution shall support secure access from unmanaged devices by routing traffic to corporate applications through the security platform for user authentication, authorisation, accounting (AAA), and comprehensive traffic inspection.

b) The solution must have the ability to allow/disallow access based on endpoint security posture, i.e. managed/unmanaged endpoint, patch level, Antivirus Patch level, Firewall, as well as customised parameters like certificates, registry entries, process lists, etc.

c) The solution shall prevent users from submitting corporate credentials to unauthorised websites based on URL categories, protecting against phishing and credential theft.

d) The solution shall inspect encrypted traffic across all ports and protocols, including SSL/TLS decryption for data centres, public clouds, SaaS applications, and the internet, to minimise security blind spots

e) The solution shall detect and protect against DNS-based threats, including DNS tunnelling, domain generation algorithms (DGAs), domain masquerading, parked domains, strategically aged domains, and DNS cache poisoning, and not be limited to DNS sinkholes.

f) The solution shall provide Intrusion Prevention System (IPS) capabilities across all ports and protocols, for both web and non-web traffic, including non-standard ports, and for all destinations (data centres, public clouds, SaaS applications, and the internet).

g) The solution shall provide Zero Trust Network Access (ZTNA), including endpoint compliance checks, user authentication, user authorisation, and continuous inspection of threats across all user-to-application traffic
h) The solution shall support external dynamic lists (EDLs) or equivalent threat feeds to automatically block malicious IP addresses, URLs, and domains, enabling automated security response.
i) The solution shall support on-site network segmentation with centralised management and integrated security inspection across segments.
j) Support application-aware traffic steering using application signatures and deep traffic inspection, in addition to Layer 3/4 attributes (IP addresses, ports, and DSCP markings).
k) The solution shall provide security capabilities across all ports and protocols, including standard and non-standard ports, for both web and non-web traffic.
l) The solution shall support packet capture upon threat detection, enabling detailed forensic analysis and incident investigation.
m) The solution shall enforce security policies based on application identification and user identity, ensuring access is granted according to each user's role and the applications they are authorised to use.
n) The solution shall restrict access to approved corporate SaaS tenants (e.g., Microsoft 365), preventing users from accessing personal or unauthorised tenants.
o) The solution shall provide inline sandboxing capabilities for traffic destined for data centres, public clouds, SaaS applications, and the internet, enabling detection and prevention of advanced threats.
p) The solution shall provide web governance and access control based on URL categories, website risk levels, phishing and malicious website detection, and application identification
q) The solution shall assign risk scores to applications based on security risk indicators to enable the identification and control of high-risk applications.
r) The solution shall support SSL/TLS decryption, including TLS 1.3, to inspect encrypted traffic for security threats across supported destinations.
s) The solution shall support creating and configuring custom security signatures to detect and prevent threats.

3.2.4. Future Capability and Functional Expansion Requirements

The proposed solution must be architecturally capable of supporting future expansion of security capabilities without requiring replacement of the core SASE platform or causing significant disruption to existing services. While the following capabilities may not be included in the initial implementation scope, the bidder must demonstrate that the proposed platform natively supports them and that they can be enabled through additional licensing, subscription, or configuration, where applicable.

a) **Cloud Access Security Broker (CASB) -** The solution must support CASB capabilities for visibility and control of sanctioned and unsanctioned cloud applications, including inline inspection and API-based integration with supported SaaS applications such as Microsoft 365 and others.
b) **Data Loss Prevention (DLP) -** The solution must support enterprise DLP capabilities, including predefined and custom data protection policies, identification of sensitive information, context-aware inspection, and

file/document matching or fingerprinting capabilities. DLP controls should be capable of being applied, where supported, across web, SaaS and private application traffic.

3.2.5. Cloud Infrastructure and PoPs

The proposed SASE solution must be delivered through a resilient, highly available cloud infrastructure that supports the BMA's distributed operations. The solution must provide the following capabilities:

a) **Local and Global Points of Presence (PoPs) -** The OEM must have operational Point(s) of Presence within South Africa to support local security inspection and minimise latency for BMA users. The bidder must provide evidence of the available South African PoPs, including redundancy and failover capabilities. The solution must also provide access to a geographically distributed global PoP network, enabling travelling users and authorised third parties to securely connect through an appropriate PoP based on their location.

b) **Multi-Cloud Support** - The solution must support secure connectivity and access to applications and services hosted across multiple cloud environments, including major public cloud providers and BMA's existing and future cloud environments, without creating unnecessary dependency on a single cloud provider

c) **Resilience and Availability** - The proposed service must provide 99.999% uptime, high availability, redundancy and automatic failover across its cloud infrastructure and PoPs. The bidder must specify the OEM's committed service availability SLA, architecture for resilience, failover mechanisms, and applicable service credits or remedies for failure to meet the committed SLA.

d) **Data Processing and Residency** – The solution must provide appropriate options for the processing, storage and retention of BMA security data and logs to support applicable South African data protection, regulatory and organisational requirements. The bidder must clearly identify where BMA data, security logs, telemetry and sandboxing data will be processed and stored, including any cross-border processing or transfer of information.

3.2.6. Platform and Policy Management

a) **Centralised Management** - Single management console for all features proposed, including policy configuration, monitoring, logging, reporting, Internet access, and administration.

b) **Granular Policy Management –** Support policies based on user, group, application, device posture, location, risk level, and time.

c) **Logging and SIEM Integration –** Support real-time monitoring, event logging, reporting, and integration with external SIEM platforms through APIs, syslog, or equivalent mechanisms.

d) **Role-Based Access Control (RBAC) –** Support role-based administrative access and separation of privileges within the management platform.

3.2.7. Deployment, Support, & Scalability

a) **Support and delivery –** The OEM must provide South African-based support and deployment services through authorised implementation partners capable of deploying the solution from start to finish, and direct support with the EOM must be available.

b) **Zero-touch Provisioning -** The solution shall support zero-touch provisioning (ZTP), enabling devices to be deployed and configured automatically with minimal manual intervention.

c) **Cloud-Native Deployment** – The solution must be cloud-native and support scalable, highly available service delivery.

d) **User Scalability** – Must support a minimum of 3,000 concurrent users across multiple locations, with the ability to scale without major architectural changes.

e) **Enterprise-ready –** The solution must be enterprise-ready and deployed with customers of similar scope and scale in South Africa

f) **Flexible Expansion –** Must support future user growth, contractors, third parties, and differentiated access requirements.

3.2.8. Reporting, Monitoring, and Visibility

a) **Monitoring and Visibility** – Provide real-time monitoring, live traffic analysis, analytics, activity logging, and security visibility.

b) **Audit Logging and Retention** – Provide comprehensive logging of user, administrative, security, and system activities, with logs retained for a minimum of 12 months. Also describe whether longer durations are possible should it be required for compliance.

c) **Dashboards and Reporting** – Provide configurable operational and executive-level dashboards and reports suitable for management and governance structures.

3.2.9. Integration Requirements

a) **Identity Integration** – Integrate with BMA's identity and access management platform, including Microsoft Entra ID, Active Directory, and support other industry-standard identity providers where required.

b) **Authentication Standards –** Support industry-standard authentication and federation protocols, including SAML 2.0, OAuth 2.0, OpenID Connect (OIDC), RADIUS, and LDAP, where applicable.

c) **MFA** – The solution must support Microsoft MFA.

d) **SIEM –** The solution must support integration with other third-party SIEM solutions.

3.2.10. Security and Access Control Requirements

a) **Traffic Protection** – Provide threat prevention and security inspection for north-south and, where supported and applicable, east-west traffic.

b) **Zero Trust Access** – Enforce secure access based on Zero Trust and least-privilege principles.

3.3. Licensing and User Capacity Requirements

The proposed Secure Access Service Edge (SASE) solution must describe the license model of the solution, with emphasis on how many devices are allowed per user in the license model, and whether the cost per user is dependent on the geographic location and country where they are based or if there is an additional fee required to use all available gateways/locations.

a) The BMA requires a license for 3000 users, with the ability to scale to accommodate future organisational growth and operational requirements.
b) Provide user-based licensing that supports access from BMA-approved desktop, laptop, and mobile devices.
c) Indicate all applicable government, enterprise, volume, or other pricing discounts applied.
d) Include all licenses, subscriptions, supporting services, and modules required to deliver the proposed SASE solution for the full contract period.
e) Include, at minimum, the following core capabilities within the proposed solution:
    - Secure Web Gateway (SWG)
    - Zero Trust Network Access (ZTNA);
    - Firewall-as-a-Service for all ports and protocols (FWaaS);
    - TLS inspection/decryption;
    - Threat Prevention and Intrusion Prevention;
    - URL Filtering;
    - Cloud-based Sandboxing;
    - DNS Security; and
    - Dedicated Egress IP capability.
    - Enterprise Browser
f) The proposed licensing must provide all dependencies required for the core capabilities specified above to operate as proposed solution should be clearly defined.
g) Be valid for a period of three (3) years from the agreed service activation date.
h) Include applicable software updates, upgrades, security and threat intelligence updates, maintenance, and OEM support for the duration of the licensing period.
i) Support cloud-delivered SASE services without requiring BMA to deploy dedicated on-premises security hardware appliances for the delivery of the proposed service, except where BMA specifically requires such deployment and discloses this requirement to the bidder.
j) Clearly describe the scalability, license thresholds, and the treatment of temporary or sustained user overages.
k) Allow BMA to increase licensed capacity and enable additional supported capabilities during the contract period, subject to applicable licensing and commercial arrangements.
l) Clearly identify which capabilities are included in the proposed license, which require additional licensing or subscriptions, and any dependencies or third-party components required.

m) CASB and DLP are future capability requirements and are not required to be licensed as part of the initial implementation. The bidder must demonstrate that the proposed SASE platform supports these capabilities and can be enabled in future, where required, without replacement of the core platform. The bidder must clearly indicate whether these capabilities are included, require additional licensing or subscription, or form part of a higher licensing tier. Provide pricing visibility for both CASB and DLP as part of the proposal.

n) Pricing and Total Cost of Ownership – Bidders must provide clear and itemised pricing covering the full three-year contract period, including all licensing, subscriptions, implementation, support, training, maintenance, and professional services required to deliver the proposed solution. Pricing must clearly identify:

- Once-off and recurring costs;
- Year 1, Year 2 and Year 3 costs;
- third-party licensing or infrastructure dependencies; and
- the total three-year contract value, inclusive of VAT.

3.4. Compliance Requirements

a) **Data Residency and Regulatory Compliance** – The solution must support data processing and residency requirements applicable in South Africa, including POPIA, National Data and Cloud Policy (NDCP), and other applicable national legislation and policies. The bidder must specify where data is stored, including metadata, policy configuration, Log Storage Management, and Sandboxing.

b) **OEM Security Assurance** – The OEM must maintain valid ISO/IEC 27001 certification and an independent SOC 2 Type II assurance report covering the proposed service.

c) **Bidder Security Assurance** – The bidder must maintain valid ISO/IEC 27001 certification applicable to the services being provided.

3.5. Training and Knowledge Transfer

a) **Technical Training** - Provide instructor-led technical training for three (3) BMA ICT Security officials covering administration, policy management, monitoring, troubleshooting, and operational management of the solution.

b) **User Awareness** – Provide end-user awareness and adoption training for designated (Train-the-trainer) BMA officials and end-user guiding documentation.

c) **Knowledge Transfer** – Provide knowledge transfer and relevant operational and configuration documentation.

3.6. Service levels, Support, and Operational Services requirements

3.6.1. The Service Provider

The bidder will be expected to provide the following service elements:

a) **Support Services** – 24/7 support for critical incidents, with appropriate technical and OEM escalation support.

b) **Incident Management** – Fault logging, tracking, escalation, communication, and resolution in accordance with agreed service levels.

c) The expected response and resolution times, based on impact and urgency:

Priority	Classification	Response Time	Target Resolution Time
P1	Critical	1 hour	2 hours
P2	High	2 hours	8 hours
P3	Medium	4 hours	48 hours
P4	Low	8 hours	96 hours

d) **Post-Implementation Support** – Provide technical support, tuning and optimisation during the agreed stabilisation period.

e) **Ongoing Support** – Provide ongoing technical and OEM support for the duration of the contract.

f) **Project Management** – Provide project management services during implementation.

3.6.2. The SASE Solution Service levels

The proposed solution uptime:

a) The BMA requires a 99.999% uptime or better, and the bidder must specify the OEM's committed service availability SLA. (Provide relevant documentary evidence)

b) The solution must provide redundancy, high availability and failover capabilities to maintain service continuity.

***NB**: The successful bidder will finalise the Service Level Agreement (SLA), including service measurement, escalation, reporting, service credits, and remedies, before services commence.*

3.7. Exit Strategy, Transition Requirements, and Expansion Capability

a) **Exit and Transition** – The bidder must provide an exit and transition approach to support the orderly migration or handover of services, configurations, applicable costs, policies, logs, integrations, and BMA data at contract termination or transition to another service provider.

b) **Infrastructure Expansion** – The solution must support the integration, migration, or addition of BMA data centres, cloud environments, and other hosting environments without requiring replacement of the core SASE platform.

c) **Service Continuity** – The bidder must describe how service continuity will be maintained during migration or expansion, including the ability to operate existing and new environments concurrently until the target environment has been tested and approved for production use.

3.8. Operating Model

a) **Co-Managed Service** – The SASE solution will operate under a co-managed model between the BMA and the service provider. BMA will retain governance, policy oversight, and decision-making authority, while BMA and the service provider will share administration and operational responsibilities under the agreed RACI matrix.

b) **Roles and Responsibilities** – The bidder must clearly define responsibilities for policy management, monitoring, incident response, change management, configuration management, escalation, and support.

c) **RACI Matrix** – The bidder must provide a RACI matrix defining the operational responsibilities of the BMA and the service provider

3.9. General and Other Requirements

a) **Industry Recognition** – The proposed SASE solution must demonstrate established industry recognition and market maturity, supported by reputable independent industry analyst reports such as Gartner, Forrester, or equivalent.

b) **Enterprise Maturity** – The solution must demonstrate proven enterprise-scale deployments and integrated policy enforcement across the proposed core SASE capabilities, with minimal reliance on third-party products for core functionality.

3.10. Bidder Technical Solution Proposal

The bidder must submit a comprehensive technical solution proposal, including all supporting annexures, certificates, OEM authorisation letters, CVs and other documentary evidence required by these Terms of Reference. **The proposal must demonstrate a clear understanding of the BMA's operational, technical and cybersecurity requirements and explain how the proposed SASE solution will address the identified challenges and meet the Scope of Work and all applicable technical and functional requirements**. Sufficient technical detail and supporting evidence must be provided to enable the BMA to assess the solution's compliance, suitability, implementation approach and overall value.

#	PROPOSAL AREA	MINIMUM INFORMATION REQUIRED
1	**Solution Architecture and SASE Platform**	Describe the proposed SASE architecture, unified management approach, traffic routing and distribution, data-plane isolation, multi-tenancy, South African and global PoPs, resilience and failover, and support for the BMA's distributed, cloud and future on-premises environments. Identify any third-party dependencies required for core SASE functionality.
2	**Core Security Capabilities**	Describe how the proposed solution delivers the core security capabilities specified in the ToR, including SWG, FWaaS for all ports and proteocls, threat prevention, IPS, anti-malware, URL filtering, application control, credential protection, DNS Security, TLS inspection, cloud-based sandboxing, Secure Enterprise Browser and Dedicated Egress IP, together with the associated security policy enforcement.
3	**ZTNA, Identity and Endpoint Context**	Describe ZTNA and secure private-application access and how it secures the BMA based on the BMA challenges and IT landscape, Microsoft Entra ID integration, authentication and federation capabilities, least-privilege access, device posture assessment and continuous user/device context. Describe support for managed and unmanaged devices and applicable leading operating systems, including Windows, macOS, iOS and Android platforms.

4	**Management, Policy and Automation**	Describe centralised management and policy enforcement across the proposed SASE capabilities, including policies based on users, groups, applications, device posture, location and risk. Describe RBAC, administrative controls and available APIs or automation capabilities for management and security operations.
5	**Logging, Monitoring, Reporting and SIEM Integration**	Describe real-time monitoring, security visibility, alerting, audit trails, log searching and retention, operational and executive dashboards (predefined and custom reports), service-status visibility and integration with external SIEM platforms through supported mechanisms such as APIs, Syslog, or any standard secure protocols.
6	**Cloud Infrastructure, Data Processing, Resilience and Availability**	Describe the South African and global PoPs supporting the BMA service; the locations where BMA data, logs, telemetry, management and sandboxing information will be processed and stored; any cross-border processing; and the proposed redundancy, failover, service availability and maintenance arrangements.
7	**Implementation, Co-Managed Operations and Support**	Describe the proposed implementation and stabilisation approach, co-managed operating model, roles and responsibilities, support model, service-level approach and RACI matrix.
8	**Licensing, Scalability and Future Capabilities**	Describe the licensing model for 3,000 users, supported devices per user, scalability, additional-user licensing, geographic/PoP restrictions or charges, licensing thresholds and dependencies. Identify capabilities included in the proposed license and those requiring separate licensing or subscriptions, and explain the treatment of temporary or sustained user overages and future expansion. Explain how CASB and DLP capabilities can be activated in future, including any additional licensing, subscription or tier requirements, without replacing the core SASE platform.
9	**Training, Knowledge Transfer and Local Delivery Capability**	Describe the proposed technical training, end-user awareness, knowledge-transfer and documentation approach, together with the local delivery and support arrangements for the proposed solution.
10	**Exit, Transition and Service Continuity**	Describe how configurations, policies, logs, integrations and BMA data can be exported or transitioned at contract termination or migration. Explain how the solution will support future BMA cloud or data-centre expansion while maintaining service continuity.

Note to Bidders: *The table below is intended as a guide to the minimum information to be included in the technical proposal. It is not exhaustive and does not replace or limit any requirement set out in these Terms of Reference (ToR). Bidders must ensure that their proposals address* ***all applicable requirements of the ToR****, including those not explicitly listed in the table, and provide the necessary supporting evidence where required.*

4. CONFIDENTIALITY OF INFORMATION

All information shared during this bidding process and, should the supplier be appointed, during the implementation of this project, remains the property of BMA and must be kept in the strictest confidence and cannot be used or shared for any other purpose.

5. PAYMENT

5.1. The supplier will be paid in South African Rands at a fixed price (Inclusive of VAT) for the service rendered.

5.2. Payment will be made within 30 days of receipt of the approved invoice, in accordance with an agreed payment schedule.

5.3. Payment will be against the key deliverables as set out in the agreed project management schedule and milestones. provided professional-level quality standards have been met. Disputes as to what constitutes a reasonable standard will be referred to an agreed provider of arbitration services.

6. RULES OF BIDDING, RFP SUBMISSION REQUIREMENTS AND EVALUATION RULES OF BIDDING

6.1 The Border Management Authority reserves to itself the right to only appoint and enter into a contractual agreement with one entity or multiple entities for the servicesrequired, which entity or entities could be an independent contractor or independent contractors or a company or companies. The appointed entity or entities will be held fully accountable for the delivery against the full terms of the contractual agreement with the BMA.

6.2 The Border Management Authority reserves the right to terminate this appointment ortemporarily defer the work, or any part thereof, should it deem necessary. Should thecontract between the BMA and the service provider be terminated by either party due to reasons not attributable to the supplier, the supplier will be remunerated for the appropriate portion of work completed up to a maximum amount of not more than the total fee quoted by the supplier for the appropriate phase of the project during which the appointment was terminated.

6.3 No data derived from the supplier for the supply of the goods under the contract may be usedfor any purposes except where authorisation in writing to do so has been granted.

6.4 The costs of preparing the bids and negotiating the contract shall be borne by the bidder, and such costs are not reimbursable. The Border Management Authority is not bound to accept any of the bids submitted and reserves the right to negotiate price(s) with the preferred bidder. The bidder may request clarification on these Terms of Reference only during the advertised period. The Border Management Authority will not accept any late submissions.

7. THE BIDS WILL BE EVALUATED AS FOLLOWS:

7.1. Stage 1: Administrative Compliance

Suppliers must ensure that the following documents are attached, signed, and completed:

(i) SBD 1: Invitation to quote/bid
(ii) SBD 3: Pricing Schedule
(iii) SBD 4 form: Bidder's Disclosure
(iv) Authority to sign the bid
(v) SBD 6.1 form: Preference Points claim form in terms of the Preferential Procurement Regulation 2022; (Note to tenderers: the tenderer must indicate how they claim for each preference point system).
(vi) SBD 7: Contract form

NB: Only bidders that meet the above requirements will be evaluated at stage two (2)

7.2. Stage 2: Mandatory Requirements

MANDATORY REQUIREMENTS	EVIDENCE OF COMPLIANCE
1. COMPLIANCE REQUIREMENTS	
1.1 The proposed Secure Access Service Edge (SASE) solution Original Equipment Manufacturer (OEM) and the bidder must hold a valid ISO/IEC 27001 certificate for Information Security Management Systems.	Bidders must submit valid ISO/IEC 27001 certificates for both the proposed OEM/OSM and the bidder. - Attached OEM/OSM ISO/IEC 27001 certificate – Information Security Management Systems (ISMS) - Attach Bidder ISO/IEC 27001 certificate – Information Security Management Systems (ISMS) If it's the EOM/OSM bidding, only submit the OEM/OSM certificate. *Note (1): BMA reserves the right to verify information provided*
1.2 The bidder must be formally authorised, accredited, or recognised by the proposed OEM/OSM to supply, resell, implement, and support the proposed SASE solution.	Bidders must submit valid documentary evidence from the OEM/OSM confirming the bidder's authorisation, accreditation, partnership, reseller status, or recognition status for the proposed SASE solution. Bidders can submit one of the following as valid evidence: - A valid OEM/OSM authorisation letter confirming that the bidder is authorised to supply/resell, implement, or support the proposed SASE solution; or - A valid OEM/OSM certificate confirming the bidder's accreditation, partnership, reseller, or recognition status for the proposed SASE solution - Or any documentation that can be validated and authenticated If the OEM/OSM is the bidder, this won't be required. *Note (1): The BMA reserves the right to verify the bidder's authorisation, accreditation, partnership, reseller, or recognition status directly with the OEM/OSM*

1.3 The OEM/OSM must have a current or most recent independent SOC 2 Type II assurance report issued in accordance with the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria.	Bidders must submit the OEM/OSM's most recent independent SOC 2 Type II assurance report for the proposed cloud-delivered security services. - Attach SOC 2 Type II Report issued in accordance with the American Institute of Certified Public Accountants (AICPA) Trust Services Criteria *Note (2): Where the most recent SOC 2 Type II report is not yet available, bidders may submit the previous SOC 2 Type II report together with a valid bridge letter issued by the OEM covering the gap between the end date of the report and the bid submission date.* *Note (1): BMA reserves the right to verify information provided*
1.4 The proposed SASE solution must provide a secure cloud service architecture supported by an operational Point of Presence (PoP) located within South Africa, ensuring that relevant security service processing, management, log storage, and cloud-delivered sandboxing are performed within South Africa.	Bidders must submit a formal letter from the OEM/OSM that confirms the location and active operational status of the South African PoP. The letter must include the following details: - Confirmation of the availability of a South African-based PoP and its active operational status - The physical or geographic location of the South African PoP - The geographic regions where sandboxing, log storage, and management services are performed, for purposes of data residency and data sovereignty verification *Note (1): BMA reserves the right to request additional technical validation, legal confirmations, or independent verification of the proposed PoP infrastructure and associated local processing arrangements during the evaluation process.*
2. BIDDER REQUIREMENTS & CAPABILITY	
2.1 The proposed Lead Security Engineer must hold a valid OEM/OSM certification for the proposed SASE solution. The Lead Security Engineer must be responsible for the implementation, configuration, and support of the proposed solution.	Bidders must submit a valid copy of the proposed Lead Security Engineer's OEM/OSM certification for the proposed SASE solution. The certification must be issued by the OEM/OSM of the proposed solution. - Attach a copy of the proposed Lead Security Engineer's OEM/OSM certification for the proposed SASE solution *Note (1): BMA reserves the right to verify the validity of the certification directly with the OEM/OSM.*
2.2 The proposed Project Manager must hold a relevant Project Management qualification or professional Project Management certification and must be responsible for managing the implementation of the proposed SASE solution.	Bidders must submit proof of the proposed Project Manager's relevant Project Management qualification, ICT qualification, Bidders must submit the following as valid evidence: - Relevant qualification as per above at NQF Level 5 or higher; *Note (1): BMA reserves the right to verify the qualification or certification with the relevant issuing authority.*

NB: Only bidders that meet the above requirements will be evaluated at stage three (3)

7.3. Stage 3: Technical Evaluation

FUNCTIONAL FACTOR	CRITERIA DESCRIPTION	SCORING METHODOLOGY	WEIGHTING
1. Experience of a Project Manager	The bidder must submit the Project Manager's CV. The Project Manager's CV must show years of experience in Project Management.	Less than 1 year **0 Points**	**20**
		1 year to less than 2 years **05 Points**	
		2 years to less than 3 years **10 Points**	
		3 years to less than 5 years **15 Points**	
		5 years or more **20 Points**	
2. Experience of Lead Security Engineer	The bidder must submit a CV for the Lead Security Engineer. The CV must show the years of experience in implementing and/or maintaining/supporting SASE/SSE solutions.	Less than 1 year **0 Points**	**20**
		1 year to less than 2 years **05 Points**	
		2 years to less than 3 years **10 Points**	
		3 years to less than 5 years **15 Points**	
		5 years or more **20 Points**	

3. Bidder SASE/SSE Implementation Experience and Client References	The bidder must provide valid reference letters from clients confirming successful implementation of SASE or SSE solutions within the past five (5) years. Each reference letter must be on the client's official letterhead and must include: a) the client's name b) A description of the scope of work performed, demonstrating that the services were related to the implementation of a SASE/SSE solution. c) The date and signature of an authorised client representative d) The name and contact details of the client representative for verification purposes.	No valid reference letters **0 Points** One (1) valid reference letter **5 Points** Two (2) valid reference letters **10 Points** Three (3) valid reference letters **15 Points**	**15 Points**
4. Solution Proposal aligned with the scope of work demonstrating clear understanding of the BMA's operational, technical, and security requirements.	The bidder must submit a technical solution proposal that addresses the ten **proposal areas specified in Section 3.10** and demonstrates how the proposed solution will meet **all the applicable requirements of the Scope of Work**. The proposal will be evaluated according to the number of proposal areas adequately addressed, the extent to which it demonstrates an understanding of the BMA's requirements and provides a technically appropriate, complete and implementable solution. A proposal area will be regarded as **adequately addressed** where the bidder responds to the minimum information required for that area and demonstrates how the proposed solution will meet the applicable detailed	No proposal submitted, or none of the 10 areas adequately addressed **0 Points** 1–2 areas adequately addressed **5 Points** 3–4 areas adequately addressed **10 Points** 5–6 areas adequately addressed **15 Points** 7–8 areas adequately addressed **20 Points**	**30 Points**

	requirements of the Scope of Work that fall within that proposal area. The response must demonstrate an understanding of the BMA's requirements and provide a technically appropriate, complete and implementable approach that is consistent with the proposed solution. An area that is merely mentioned, contains generic marketing information, does not address the applicable detailed ToR requirements, or has material omissions will **not** be counted as adequately addressed.	9 areas adequately addressed **25 Points** All 10 areas adequately addressed **30 Points**	
5. The proposed solution is recognised in the Independent Industry analyst reports for SASE solutions.	The proposed solution must demonstrate established industry recognition and market maturity through inclusion in the latest available assessment cycle for each qualifying independent industry analyst publication that directly evaluates SASE or Security Service Edge (SSE) Recognised publications may include reports issued by Gartner, Forrester, IDC. SecureIQLab, or another equivalent reputable independent industry analyst organisation. A qualifying report must: • Be issued by an independent and established industry analyst organisation; • Directly evaluate multiple competing SASE, SSE or equivalent solutions; • Assess the proposed OEM solution rather than only the bidder or managed service provider; • Be from the latest available assessment cycle for that publication; and • Provide verifiable evidence of the proposed solution's inclusion and, where applicable, positioning.	The proposed solution is not included in any qualifying analyst report, or verifiable evidence is not provided. **0 Points** The proposed solution is included in one (1) qualifying analyst report. **3 Points** The proposed solution is included in qualifying analyst reports issued by two (2) distinct independent analyst organisations. **6 Points** The proposed solution is included in qualifying analyst reports issued by three (3) or more distinct independent analyst organisations. **9 Points** The proposed solution is included in qualifying	**15 Points**

	Highest applicable category means the highest vendor category, tier or position assigned under the report's published methodology. Where a report does not assign categories or comparative positioning, it will count only as evidence of inclusion. For scoring purposes, reports must be issued by distinct independent analyst organisations. Where the proposed solution qualifies for more than one scoring band, the highest applicable score will be awarded. The bidder must provide the relevant extract, publication details or an accessible reference sufficient for the BMA to verify the report, publication date, evaluated market and the proposed solution's inclusion and positioning.	analyst reports issued by three (3) or more distinct independent analyst organisations and is positioned in the highest applicable category in one (1) qualifying report. **12 Points**	
		The proposed solution is included in qualifying analyst reports issued by three (3) or more distinct independent analyst organisations. It is positioned in the highest applicable category in three (3) or more qualifying reports. **15 Points**	
TOTAL			**100**
The Technical Qualification Threshold is 75.			

7.4. Stage 4: Demonstration

Bidders who meet the Stage 3 requirements will be invited to demonstrate the proposed SASE solution. The demonstration aims to validate that the proposed solution can deliver the key security, access, management, monitoring, and operational capabilities required by the BMA.

The demonstration must use the actual proposed OEM solution in a live demonstration or functional controlled environment. PowerPoint presentations, product brochures, prerecorded demonstrations, historical events or verbal confirmation alone will not constitute demonstration of functionality. For threat scenarios, bidders must use safe test files or domains, platform-generated test events or controlled test traffic and show the resulting enforcement action, logs, alerts or reports in the proposed platform. Live malicious software must not be introduced.

Bidders will receive the final demonstration script and at least two (2) weeks' notice. The same scenarios, instructions and time allocation will apply to every bidder. The proposed OEM may support the bidder.
The bidder must demonstrate the following scenarios:

#	DEMONSTRATION SCENARIO	CAPABILITIES TO BE DEMONSTRATED	TOTAL SCORE
1	**Centralised Management, Administration and RBAC**	(1) Use the unified console to configure a policy; (2) administer the proposed SASE components; (3) demonstrate separation of administrative privileges; and (4) display the resulting administrative audit trail. **Scoring:** **Fully demonstrated = 8 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 4 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	**8**
2	**Identity, MFA, Device Posture and Contextual Access**	(1) Authenticate a test user; (2) demonstrate identity integration and MFA capabilities; (3) apply user/group, location, application and risk conditions; (4) apply representative device-posture conditions; and (5) show allow and deny outcomes for managed and unmanaged test devices. **Scoring:** **Fully demonstrated = 12 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 6 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	**12**
3	**User Experience and Operational Usability**	Assess the usability observed across the demonstration, including: (1) ease and clarity of the end-user experience; (2) ease and clarity of the administrator workflow; (3) service-status visibility; and (4) availability of basic operational troubleshooting information. (5) Demonstrate Digital Experience Management (DEM) capabilities **Scoring:** **Fully demonstrated = 4 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 2 points:** At least half of the listed	**4**

		capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	
4	**ZTNA and Private Application Access**	(1) Provide an authorised test user with least-privilege access to a test private application; (2) Demonstrate that there is no VPN connection; (3) deny an unauthorised user; and (4) show the user/device context, inspection result and related logs. **Scoring:** **Fully demonstrated = 14 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 7 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	**14**
5	**Secure Enterprise Browser**	(1) Use the secure enterprise browser to access a test SaaS or private web application; (2) demonstrate representative session controls; (3) demonstrate representative data controls on a managed or unmanaged test device; and (4) where supported by the proposed capability, demonstrate access without the endpoint SASE agent. **Scoring:** **Fully demonstrated = 8 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 4 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	**8**
6	**Secure Web Gateway, URL and SaaS Controls**	(1) Inspect test web traffic; (2) configure and enforce URL category, reputation or risk controls; (3) configure and enforce a custom allow/block policy; (4) use test credentials to demonstrate credential protection; (5) show application identification and risk; and (6) restrict access to an unauthorised test SaaS tenant. **Scoring:** **Fully demonstrated = 12 points:** All listed capabilities are	**12**

		demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 6 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	
7	**TLS Inspection and Policy Enforcement**	Using representative supported traffic: (1) demonstrate TLS 1.3 inspection; (2) configure and apply a policy-based decryption rule; (3) demonstrate a decryption exclusion; and (4) show the visible inspection or policy results in the proposed platform. **Scoring:** **Fully demonstrated = 8 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 4 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	**8**
8	**DNS Security, Threat Prevention and Sandboxing**	Using safe test domains or files, platform-generated test events or controlled test traffic: (1) demonstrate detection or blocking of representative DNS threat activity (DNS inspection traffic capabilities not just DNS sinkhole); (2) demonstrate detection or blocking of representative malware, IPS or command-and-control activity; (3) show inline sandbox submission and the available verdict; (4) show the resulting enforcement action and alert; and (5) show the resulting logs or forensic evidence. **Scoring:** **Fully demonstrated = 12 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 6 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	**12**

9	**FWaaS, Application Control and Dedicated Egress IP**	(1) Configure and enforce a Layer 7 or identity-aware firewall rule; (2) identify and control a test application on a standard or non-standard port; (3) show the visible static or dedicated egress IP; and (4) show the related policy result. **Scoring:** **Fully demonstrated = 10 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform. **Partially demonstrated = 5 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	**10**
10	**Logging, Monitoring, Reporting and SIEM Integration**	(1) Generate and locate a live test event; (2) demonstrate alerting, search and filtering across relevant logs; (3) show the configured retention control; (4) display operational and executive dashboards; (5) generate and export a report; and (6) demonstrate SIEM integration capabilities within the centralised management console. **Scoring:** **Fully demonstrated = 12 points:** All listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform or receiving test endpoint. **Partially demonstrated = 6 points:** At least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations. **Not demonstrated = 0 points:** Fewer than half of the listed capabilities are demonstrated.	**12**
TOTAL			**100**

Scoring: Each scenario will be scored using the three levels stated in the scenario row:

- **Fully demonstrated** where all listed capabilities are demonstrated, and the results are visible and verifiable in the proposed platform;
- **Partially demonstrated** where at least half of the listed capabilities are demonstrated and verifiable, but one or more capabilities are not demonstrated or contain material limitations; and
- **Not demonstrated** where fewer than half of the listed capabilities are demonstrated. Where the listed capabilities cannot be divided equally, the minimum required for a partial score will be rounded up to the next whole capability.

NB: Only bidders that achieve the minimum Stage 4 demonstration threshold of 75 out of 100 points will proceed to Stage 5: Price and Specific Goals Evaluation.

7.5. Stage 5: Price and Specific Goals Evaluation

Preferential Procurement Evaluation Based On The 80/20 Principle

The applicable formula (80/20) will be utilised to evaluate the bid, of which eighty (80) points are allocated for price as allocated in the enclosed form SBD 6.1. that must be completed, and the remaining twenty (20) points are allocated for the specific goals as indicated in the table below

Responsive bids will be adjudicated by the State on the 80/20 preference point claim in terms of the Preferential Procurement Regulation 2022 which points are awarded to bidders based on:

The bid price (maximum 80 points)

Specific Goals (maximum 20 points)