THE BORDER MANAGEMENT AUTHORITY (BMA) INVITES ALL INTERESTED PARTIES TO RESPOND TO THE REQUEST FOR PROPOSAL (RFP) FOR THE IMPLEMENTATION OF AN INTERACTIVE ADVANCED PASSENGER INFORMATION (iAPI), PASSENGER NAME RECORD (PNR) AND PASSENGER RISK ENGINE WITH TARGETING TOOL FOR A PERIOD OF FIVE (5) YEARS

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 **14 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	DECLARATION OF INTEREST
SECTION G	PREFERENCE POINTS CLAIM FORM (SBD6.1)
SECTION H	CONTRACT FORM (SBD 7)
SECTION I	CONDITIONS OF BID
ANNEXURE B	GENERAL CONDITIONS OF CONTRACT (GCC)
SECTION J	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:	**H004L2710RFP00198**	**CLOSING DATE:**	**14 DECEMBER 2026**	**CLOSING TIME:**	**11H00**
DESCRIPTION	**THE BORDER MANAGEMENT AUTHORITY (BMA) INVITES ALL INTERESTED PARTIES TO RESPOND TO THE REQUEST FOR PROPOSAL (RFP) FOR FOR THE IMPLEMENTATION OF AN INTERACTIVE ADVANCED PASSENGER INFORMATION (iAPI), PASSENGER NAME RECORD (PNR) AND PASSENGER RISK ENGINE WITH TARGETING TOOL FOR A PERIOD OF FIVE (5) YEARS**				
BID DOCUMENTS ARE TO BE SUBMITTED THROUGH E-TENDER PORTAL (E-SUBMISSIONS)					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO			**TECHNICAL ENQUIRIES MAY BE DIRECTED TO:**		
CONTACT PERSON			**CONTACT PERSON**	**Neo Mampa**	
TELEPHONE NUMBER			**TELEPHONE NUMBER**	**N/A**	
E-MAIL ADDRESS	suppliers.enquiries@bma.gov.za		**E-MAIL ADDRESS**	Neo.mampa@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 66 TO 67
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: Contract Form	

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 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

[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.

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 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 G
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 90/10 preference point system.

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	**90**
SPECIFIC GOALS	**10**
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**

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

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.) Attach active BBBEE certificate or Affidavit

The specific goals allocated points in terms of this tender	Number of points allocated (90/10 system) (To be completed by the organ of state)	Number of points claimed (90/10 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 = 5 **points** • ≥51% and <100% company owned by people who are Black = 3 **points** • >0% and <51% company owned by people who are Black = **2 points** • 0% of companies owned by people who are Black = **0 points**	5	
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 Women = **0 points**	3	
The company is owned / director/s / shareholders by people who are Youth. • 100% company owned by people who are Youth = 2 **points** • ≥51% and <100% company owned by people who are Youth = 1 **points** • 0% and <51% company owned by people who are Youth = 0 **points**	2	

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 H
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 **H004L2710RFP00198** 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 I

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 J

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: H004L2710RFP00198

SERVICE: THE BORDER MANAGEMENT AUTHORITY (BMA) INVITES ALL INTERESTED PARTIES TO RESPOND TO THE REQUEST FOR PROPOSAL (RFP) FOR FOR THE IMPLEMENTATION OF AN INTERACTIVE ADVANCED PASSENGER INFORMATION (iAPI), PASSENGER NAME RECORD (PNR) AND PASSENGER RISK ENGINE WITH TARGETING TOOL FOR A PERIOD OF FIVE (5) YEARS.

****

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 C

TERMS OF REFERENCE

THE SERVICE PROVIDERS TO RESPOND TO THE REQUEST FOR PROPOSAL (RFP) FOR THE IMPLEMENTATION OF AN INTERACTIVE ADVANCED PASSENGER INFORMATION (iAPI), PASSENGER NAME RECORD (PNR) AND PASSENGER RISK ENGINE WITH TARGETING TOOL FOR A PERIOD OF FIVE (5) YEARS.

1. Background

The Border Management Authority (BMA) was formally established as an autonomous national public entity on 1 April 2023. Its mandate includes facilitating and managing the legitimate movement of persons and goods at Ports of Entry and within the border law-enforcement area, while coordinating border law-enforcement functions with relevant organs of state and stakeholders. Effective delivery of this mandate depends on timely, reliable and secure passenger information that enables authorised officials to identify risk before a traveller reaches the border or commences a journey to South Africa.

South Africa has operated an interactive Advance Passenger Information (iAPI) capability, known as Advanced Passenger Processing (APP), since the period preceding the 2010 FIFA World Cup however PNR compliance is required by the United Security Council Resolution 2396 01 which places an obligation on UN Member States to develop a PNR capability. That capability established an important foundation for advanced traveller screening. The BMA now requires a modern, integrated and supportable platform that combines iAPI, Passenger Name Record (PNR) information, passenger risk assessment and targeting in a single operational environment.

The proposed solution must support the increasing volume, speed and sensitivity of passenger and crew information across air and maritime operations, while providing a scalable path for rail and bus operations. It must strengthen advanced decision-making, improve the quality and traceability of screening outcomes, support carrier compliance and provide the resilience required for continuous national border operations.

Current-state context

The existing iAPI capability supports advance screening of international travellers and crew (in the air and maritime environment), however PNR is required in support of global best practices for use of this data for law enforcement, aviation and maritime security, border control / management and counterterrorism purposes primarily in the air and maritime modalities. The procurement will modernise this capability, introduce integrated PNR processing and risk-based targeting, and establish BMA-owned private-cloud infrastructure across primary and recovery environments. The resulting service must operate as one end-to-end capability, with clear accountability for carrier connectivity, data processing, security, implementation, support and continuity.

Strategic intent

Strengthen the BMA's ability to identify known high-risk people before travel commences and to support timely, lawful intervention.

Enable authorised officials to identify previously unknown persons of interest through configurable business rules, behavioural indicators and risk profiles.

Establish a scalable, resilient and secure passenger information platform for long-term national border operations across air, maritime, rail and bus modalities.

Purpose

The purpose of this document is to define the requirements for appointing a suitably qualified service provider to supply, implement, integrate, operate, support and maintain a fully integrated iAPI, PNR, passenger risk engine and targeting solution for a period of five (5) years.

Objective

The objective is to enable advance identity and risk assessment of arriving, departing and transiting international passengers and crew, and to support real-time or near-real-time intervention before boarding or arrival where required.

Primary objectives

i) Receive and process iAPI and PNR information from participating carriers in accordance with applicable international passenger data standards.
ii) Expand the existing capability from traditional API processing to integrated iAPI and PNR processing with advanced passenger risk analysis and targeting capability.
iii) Support aviation and cruise or maritime passenger processing, with the capability to extend passenger processing to land and rail environments while maintaining border security and traveller facilitation.
iv) Provide an electronic gateway for airlines, cruise, bus and rail operators to transmit required passenger, crew and journey information to the BMA.
v) Return real-time boarding directives to carriers through their Departure Control Systems (DCS).
vi) Combine passenger data, travel history, PNR, flight/cruise/travel and screening results into a coherent operational profile.
vii) Allow for risk analysis/assessment, watchlist, targeting, enquiry, reporting and audit capabilities.

Desired outcomes

i) Earlier identification of inadmissible or high-risk travelers.
ii) Improved decision-making through data-driven analytics and targeting
iii) Greater operational resilience, traceability, security and regulatory compliance.
iv) A supportable platform with controlled technology refresh over the contract term.
v) Efficient compliance with border-management legislation, applicable standards, good practice and regulatory requirements.

Scope

Scope of Intent

i) Interactive API processing and real-time boarding directives (software).
ii) Passenger Name Record acquisition and reconciliation (software).
iii) Integration of airlines, cruise lines, rail operators and bus operators, including passenger and crew data acquisition.
iv) Risk assessment, targeting, watchlists and analytics, with the capacity to interface with operational systems such as movement control and electronic travel authorisation.
v) Procurement and implementation of secure primary and recovery infrastructure for a BMA-owned private cloud.
vi) Cybersecurity, testing, compliance and auditable transaction records.
vii) Data migration from the existing data centre to the new environment, including reconciliation, training, cutover and operational readiness.
viii) Accessible and efficient user functionality that supports operational navigation, decision-making and user experience.
ix) 24/7/365 support, maintenance, service-level management and controlled technology refresh.

Scope of Service

The appointed supplier will be responsible for the full lifecycle of the iAPI/PNR capability: solution design, supply, hosting/infrastructure, carrier connectivity, integration, configuration, implementation, migration, testing, commissioning, training, cutover, operations, support, maintenance, security, reporting and technology refresh.

In-scope service domains

i) Passenger and crew data acquisition from airlines, cruise lines, rail operators and bus operators.
ii) iAPI transaction processing and boarding directives.
iii) PNR ingestion at defined intervals and reconciliation with iAPI/manifest information.
iv) Processing flight, voyage, rail and bus arrival and departure information.
v) Flight, voyage and crew information processing.
vi) Risk assessment, targeting, watchlists, rules, profiling and analytics, including interoperability with systems such as electronic travel authorisation and movement control.
vii) BMA user access, enquiry, case-supporting searches, reporting and audit trails.
viii) Primary and recovery environments, network connectivity and BMA-owned private-cloud infrastructure.
ix) Cybersecurity, monitoring, backups, resilience and operational support.
x) Accommodate Change Requests when the need arise.

Functional Requirements

Carrier Integration and Data Acquisition

A central requirement is the secure, bidirectional acquisition of passenger, crew and journey information from carriers and operators across air, maritime, rail and bus modalities. The supplier must provide the connectivity, messaging and integration services required for carriers to transmit data to the BMA and receive responses through their operational systems.

Data Acquisition System (DAS)

Validate inbound messages before forwarding them to the iAPI/PNR targeting environment.

Handle the expected formats and standards used by airline, cruise-line, rail and bus reservation, departure-control and operating systems.

Detect missing, late, malformed, duplicate or otherwise exceptional messages and alert the BMA.

Provide full traceability for transmissions, responses, failures and retries, including unique messaging identifiers, timestamps and status codes.

Carrier onboarding

Plan and execute the onboarding of all commercial airlines, cruise lines and any other carriers designated by the BMA, including rail and bus operators.

Coordinate interface testing, certification and production cutover with each carrier according to an agreed schedule.

Maintain integration documentation, contact points, schedules and operational support arrangements, and make this available to the BMA on request.

Secure transport

Use mutually authenticated, encrypted interfaces and secure messaging mechanisms that meet or exceed best practices on cryptographic standards.

Protect confidentiality, integrity and authenticity of passenger data in transit at rest and in use.

Passenger Name Record (PNR) Requirements

PNR is declarative reservation and itinerary information obtained from airline reservation and departure control systems. The solution must receive, validate, standardize, store, reconcile and use PNR information for advance risk assessment.

Transmission timing

Support updated PNR information at least 72, 24 and 8 hours prior to scheduled flight departure.

Support an update at check-in, where PNR is merged with iAPI and boarding pass information.

Support final updates at departure/flight close.

Support BMA-approved transmission schedules for maritime, rail and bus departures, aligned with operational and regulatory requirements.

Data quality and standards

Use BMA-approved formats aligned with recognised industry standards, including applicable ICAO, IATA and WCO passenger-data message standards.

Validate completeness, timeliness and format before downstream screening.

Alert the BMA when PNR is erroneous, late, not received or cannot be processed, with sufficient detail for operational response.

Operational use

Send validated PNR information to the risk engine for screening.

Reconcile PNR with iAPI/manifest information to form a holistic traveler profile.

Retain transmission and screening history for audit and enquiry in accordance with BMA-approved retention rules.

Interactive Advance Passenger Information (iAPI)

iAPI captures passenger biographical and travel document information during check-in and exchanges it interactively with the BMA so that a boarding directive can be returned to the carrier's DCS.

Interactive processing

Receive iAPI on a per-passenger basis during check-in, including kiosk and online check-in where supported.

Screen the passenger against watchlists, rules and risk criteria in real time.

Return a BMA-approved boarding directive, including "Board", "No Board" or other ICAO-compliant messages.

Directive control

Allow directives to be generated automatically using configurable rules, issued using an approved default, or escalated for authorized manual intervention.

Notify the BMA if the directive fails to reach the carrier within the agreed time.

Maintain a full audit trail of request, decision, rule hit, user intervention and response.

Analyse failed or delayed directives to identify technical, process and data-related causes, and generate reports showing root causes, trends and recommended corrective actions.

Performance

The end-to-end turnaround from capture at check-in to receipt of the boarding directive at the carrier shall not exceed ten seconds under agreed operating conditions.

Flight, Crew, Cruise, Bus, Rail and Manifest Processing

The system must support passenger and crew movements across international air, cruise, rail and bus operations and maintain journey-level context for targeting, reconciliation and operational decision-making.

Flight and voyage information

Receive and maintain route, carrier, departure, arrival, port-of-last-call and other relevant journey information.

Associate each passenger/crew record with the applicable journey and movement event.

Support arriving, departing and transiting movement scenarios.

Flight/Cruise/Rail and Bus manifest

Receive consolidated iAPI/manifest information after departure within a BMA-approved timetable.

Reconcile final manifest data with previously received PNR and interactive API transactions.

Identify inconsistencies such as checked-in but not boarded, boarded without expected prior records, or data mismatches.

Crew processing

Process required crew information using the same security, timeliness, validation and risk assessment and audit principles applicable to passenger information.

Risk Assessment, Targeting and Watchlists

The iAPI/PNR platform must provide a robust risk engine that enables the BMA to identify known threats and discover previously unknown persons of interest through configurable analytical and targeting capabilities. This risk engine and targeting capability should be able to interface with other business systems, such as the Movement Control Systems and the Electronic Traveller Authorisation (ETA) system, in support of a single risk engine and targeting solution.

Risk models

Support Known Risk, Behavioral Risk and Random Risk assessment approaches.

Enable exploratory, predictive and other analytics appropriate to the available data and approved use cases.

Provide a controlled configuration environment that allows authorised BMA users to create, test, approve, version and deploy business rules, thresholds, profiles and targeting criteria.

Configuration changes shall follow a defined workflow with segregation of duties, impact assessment, testing in a non-production environment and a complete audit trail.

Watchlists

Create, maintain and screen against watchlists manually and automatically.

Support fuzzy matching and identity resolution to reduce evasion through minor data manipulation.

Generate alerts when a match or qualifying risk condition occurs, categorize each match as Critical, High, medium or Low according to BMA configurable criteria, and retain the basis for the alert (including the matching fields, score and rule/watchlist identifier).

Governance

Apply role-based control to rule creation and approval.

Maintain version history and auditability of rules, profiles and watchlists.

Provide explainable screening results sufficient for operational decision-making and audit review.

User Management, Search, Enquiry and Reporting

The system must provide authorized BMA users with secure, efficient access to passenger, crew, flight, cruise, rail and bus screening and operational information while maintaining segregation of duties and auditability.

User management

Provide role- and group-based access control and explicit assignment of privileges.

Support administrative functions for user provisioning, privilege management and access reviews.

Automatically terminate inactive sessions after a configurable period.

Search and enquiry

Support case-insensitive, exact, key, wildcard, multi-parameter and range searches.

Allow authorized users to enquire across passengers, crew, journey, risk, watchlist and transaction information.

Provide controlled data maintenance functions for approved reference data and parameters.

Reporting

Provide predefined management/statistical reports and a user-friendly ad hoc report generator.

Support tables, dashboards and graphical outputs with export to common office/document formats (pdf, word, excel, etc.).

Generate detailed screening, exception, cross-reference, user activity and audit reports on scheduled or on-demand cycles.

Data Management, Retention and Migration

The solution must manage passenger and operational data as a controlled enterprise information asset throughout its lifecycle.

Database and scalability

Use an open, modular and scalable enterprise-class data architecture.

Minimize unnecessary duplication and support expected growth, including an indicative annual database growth assumption of approximately 10%.

Support high-volume concurrent transactions and future expansion.

Retention and archiving

Store required inbound and outbound information and screening results in accordance with BMA-approved retention rules.

Archive records that exceed active retention periods and support authorized modification of retention settings.

Apply data masking or anonymization where required for archived or non-production use.

Data Migration

Provide and execute a detailed data migration plan covering extraction, mapping, transformation, cleansing, loading and validation.

Document source-to-target field mappings and obtain BMA approval before excluding any data.

Protect data during migration and verify completeness, accuracy and integrity before acceptance.

Solution Architecture — High-Level Principles

The solution architecture must support national-scale, mission-critical passenger processing and remain supportable throughout the five-year contract period.

Architecture principles

Integrated end-to-end solution with consistent navigation, security and operational management.

Modular and scalable design that can accommodate increased transaction volumes, users, carriers and data sources.

No single point of failure in critical processing paths.

Separation of production, test/development and management environments.

Standards-based interfaces and technologies that support interoperability and controlled future change.

Primary and secondary environments

Provide a primary production environment and a secondary/DR environment.

Maintain data synchronization and automatic or controlled failover consistent with approved recovery objectives.

Describe conditions in which automatic failover is not feasible and provide mitigation and recovery procedures.

Documentation

Provide logical, physical, security, data and integration architecture diagrams and maintain them under configuration control.

Infrastructure and BMA Private Cloud

The bidder must procure, supply, deliver, install, configure, commission and support all infrastructure required for the solution. The infrastructure, software licenses and associated management components procured under this tender shall be owned by and registered in the name of the BMA. The bidder shall not provide the production or recovery environment as a shared public-cloud or supplier-owned hosting service.

Hosting model and locations

The solution shall be deployed as a dedicated BMA private cloud comprising a primary data center and a geographically separated recovery data center. The BMA will determine and approve the physical locations during contracting. Both locations shall be within the Republic of South Africa.

The bidder shall include all infrastructure, software, subscriptions, installation services, warranties, maintenance and technical support needed for the full five-year contract period.

The bidder shall clearly identify any component that is licensed rather than owned and shall ensure that such licensing does not limit the BMA’s access to its data, configurations or operational records.

High-level infrastructure sizing

The proposed private cloud shall be sized from verified passenger, crew, PNR, iAPI, journey, watchlist, audit, security-log and reporting volumes. The design shall support the anticipated five-year data growth, peak travel periods and at least thirty percent capacity headroom at final acceptance. The bidder shall submit detailed sizing calculations and assumptions covering compute, memory, storage, network throughput, input and output operations, retention, backup, replication and disaster recovery.

The solution shall support an indicative minimum of **15 million** passenger or crew movement and reservation-related records per year, together with all associated versions, messages, screening results, alerts, audit records and operational logs. This figure is a sizing baseline

and not a volume guarantee. Final sizing shall be validated during inception without reducing the bidder's obligation to provide a complete and scalable solution.

Compute and virtualization

The private cloud shall use enterprise-class, redundant compute nodes with no single point of failure. It shall support virtual machines and containerized workloads where required, automated workload restart, resource pooling, live workload mobility, high availability and central lifecycle management. Processor, memory and node quantities shall be justified through the sizing model and shall allow non-disruptive expansion.

Storage and data protection

The bidder shall provide enterprise storage suitable for high-volume transactional databases, message processing, analytics, document or object storage, security logs, backups and archives. The architecture shall use appropriate high-performance and capacity tiers, encryption at rest, data integrity controls, snapshots, replication, immutable or logically isolated backup copies and scalable retention. Storage shall be sized on usable capacity after protection overheads, not raw capacity.

The bidder shall propose a backup architecture providing application-consistent and database-consistent recovery, protection from unauthorized deletion or ransomware, and periodic restoration testing. Backup administration shall be protected through multi-factor authentication and segregation of duties.

Network and security infrastructure

The bidder shall provide redundant switching, routing, load-balancing and security infrastructure for both data centres, including the required interfaces to the BMA, the Department of Home Affairs, carriers and other authorised government or partner systems. The design shall segregate management, application, database, storage, backup, replication, security and external-integration traffic. All critical paths shall be redundant and capable of automatic or controlled failover.

The private cloud shall include next-generation perimeter and internal segmentation firewalls, secure remote administration, privileged-access controls, multi-factor authentication, vulnerability management, central log collection, security monitoring and integration with the

BMA security operations capability. Administrative and monitoring tools shall be licensed for the full environment.

Primary and recovery data centres

The primary and recovery environments shall have sufficient capacity to process critical production workloads following failover. The bidder shall state any differences between the sites and demonstrate that these differences will not prevent achievement of the approved recovery objectives. Data, application configurations, security controls, rules and required logs shall be replicated according to the approved recovery design.

The design shall target a recovery time objective not exceeding sixty (60) minutes and a recovery point objective not exceeding fifteen (15) minutes for critical services. Durable messaging and reconciliation shall prevent avoidable loss of iAPI and PNR transactions. The bidder shall conduct quarterly technical failover tests and at least one full end-to-end disaster recovery exercise annually, with reports and corrective actions submitted to the BMA.

Management support and technology lifecycle

The bidder shall provide central monitoring and management for compute, storage, networks, virtualization, databases, backups, replication, operating systems and security. The BMA shall receive full administrative visibility and access consistent with segregation of duties. Monitoring shall cover availability, utilization, performance, capacity, hardware health, replication, backup status, security events and license status.

All infrastructure shall be current, supported and covered by original manufacturer warranties and support for the required term. The bidder shall provide a technology refresh and end-of-support plan, maintain configuration and asset registers, label all equipment and cabling, and transfer all warranties, licenses, subscriptions, documentation and support entitlements to the BMA.

Infrastructure deliverables and acceptance

Infrastructure acceptance shall require approved detailed design, bills of materials, factory or supplier test evidence, delivery and asset verification, installation, configuration, security hardening, performance and capacity testing, backup restoration, replication and failover

testing, as-built documentation, operating procedures, training and formal BMA sign-off. Payment for infrastructure shall be linked to verified delivery and acceptance milestones.

Performance, Capacity, Availability and Resilience

The system is a mission-critical border processing capability and must maintain predictable performance under normal, peak and degraded conditions.

Availability

Operate continuously on a 24/7/365 basis.

Cloud and managed services shall achieve at least 99.9% uptime unless a higher service level is agreed for critical components.

Planned maintenance shall be controlled to minimize operational impact.

Performance

Meet the iAPI boarding directive turnaround requirement and BMA-approved response times for enquiry, reporting and operational functions.

Size the platform for peak concurrent transactions and expected future growth.

Ensure reporting and audit activity does not materially degrade real-time passenger processing.

Resilience

Design for redundancy across critical application, database, network, storage and security components.

Support graceful recovery, data consistency and failover without unnecessary system restart or re-boot.

Monitor capacity, failure events and degradation trends and take proactive corrective action.

System Interfaces and Integration

The bidder is responsible for all interfacing and integration required between the iAPI/PNR solution, carriers and BMA-authorized internal or external systems. This responsibility includes passenger and crew data flows.

Integration principles

Use documented, standards-based interfaces and mutually authenticated secure communications.

Define data ownership, format, field mapping, protocol, frequency, error handling and reconciliation for each interface.

Isolate integration failures so that one external system does not cause uncontrolled failure of the core platform.

Interface management

Maintain an interface catalogue and detailed interface control documents.

Provide monitoring, message tracking and exception queues for all critical interfaces.

Support controlled changes to interfaces through configuration and change management processes.

Security

Encrypt sensitive information in transit, rest and in use.

Use secure Application Programming Interface gateways and messaging gateways where appropriate.

Restrict interfaces to authorized endpoints and approved traffic flows.

Cybersecurity — Governance and Control Framework

Security is a foundational requirement because the solution processes sensitive passenger and border security information. The supplier must implement defense-in-depth controls covering people, process, technology and third parties.

Security governance

Comply with BMA security policies, written security instructions and approved security baselines.

Maintain system-specific security architecture, security plan, roles, responsibilities, operating procedures and configurations.

Extend applicable security obligations to subcontractors and third parties.

Obtain and provide to the BMA, on request, evidence of periodic compliance verification of subcontractors and third parties that process or have access to BMA data or systems.

Core control objectives

Authentication, authorisation, accountability and non-repudiation.

Confidentiality, integrity and availability of information and services.

Prevention and detection of unauthorized access, malware, data loss, tampering and hidden functionality.

Security lifecycle

Apply security from design through development, testing, commissioning, operation, change and decommissioning.

Remediate security flaws identified during reviews, tests or audits within BMA approved timeframes according to severity and provide evidence of remediation.

Identity and access management

Provide IAM with multi-factor authentication for appropriate user classes.

Implement role-based access control and segregation of duties.

Grant rights explicitly and review access periodically.

Support defined user classes such as operational users, supervisors and system administrators/super users.

Privileged access

Provide and monitor privileged access management with controlled sessions and recording where required.

Use separate privileged and normal user accounts for administrators.

Protect remote administration using BMA-approved access controls and network restrictions.

Credential controls

Enforce strong password and session policies, account lockout and secure credential storage.

Protect authentication information in transit and at rest; credentials must never be transmitted in clear text.

Application, API and Data Security

Application and data-layer security must protect the solution against common and advanced attack patterns while ensuring integrity of passenger decisions.

Application security

Use a multi-tier architecture that separates presentation, session control, business logic and database access.

Apply input/output validation, workflow controls, message integrity and secure exception handling.

Protect against broken access controls, injection, cross-site scripting, insecure storage/configuration, denial of service and related vulnerabilities.

API and messaging security

Use a secure API gateway and secure iAPI/PNR messaging gateway.

Authenticate endpoints and protect messages against interception, alteration and replay.

Implement rate limiting, filtering and monitoring appropriate to high-volume border processing.

Data protection

Encrypt data at rest and in transit using BMA-approved cryptographic controls.

Implement certificate and key management, data loss/leak prevention, masking, tokenization and anonymization where appropriate.

Preserve referential integrity when masking data across related records.

Security Monitoring, Audit Logs and Time Synchronization

The BMA must be able to reconstruct security and operational events and identify malicious or anomalous behavior across the full solution stack.

Centralized monitoring

Provide SIEM and, where applicable, user/entity behavior analytics.

Aggregate application, operating system, database, security, network and backup logs.

Provide SOC analysis capability and escalation processes appropriate to the agreed service model.

Audit records

Capture successful and failed logins, privileged use, access violations, service start/stop, backup/recovery events, configuration changes and anomalous events.

Protect audit trails against unauthorized deletion or modification and maintain them in human-readable form.

Record sufficient identity, source, destination, event, action and timestamp details (who / what / how / when).

Time synchronization

Synchronize system devices to a BMA-approved authoritative time source to ensure consistent audit chronology.

Security Assurance, Testing, Audit and Compliance

Security controls must be independently testable and subject to BMA oversight throughout the contract

.

Security assessment

Conduct risk-based security reviews before commissioning and for significant enhancements.

Support host, network and web application vulnerability scanning, penetration testing and source code review/scanning where applicable.

Resolve identified security weaknesses before production acceptance or within BMA-approved risk treatment timelines.

Allow for independent security assessment to be conducted on the established ICT environment.

Audit rights

The BMA retains the right to conduct ad hoc audits of the supplier and relevant subcontractors.

The supplier shall provide information, assistance and evidence and implement approved recommendations within agreed timeframes.

Compliance

Comply with applicable legislation, regulation, contractual obligations and BMA security policies.

Protect important records from loss, destruction and falsification.

Ensure personnel and subcontractors understand and comply with security responsibilities.

Software Platform and Licensing Requirements

The software stack must be supportable, secure, integrated and licensed for the intended operational scale.

Software principles

Use supported commercial software and/or approved open-source components.

For open-source components, identify usage, support ownership and vulnerability management responsibilities.

Provide a logical function hierarchy showing relationships between modules.

Maintain consistent user experience across integrated third-party components.

Versions and updates

Supply current supported software versions unless a justified exception and upgrade roadmap is approved.

Test patches, anti-malware updates, OS/database updates and software upgrades in non-production before deployment.

Apply updates without unnecessary service interruption.

Licensing

Provide sufficient server, client, concurrent, enterprise or site licenses as appropriate for all required environments (production, DR, test and training).

Ensure licensing remains valid for the full contract period, warranty obligation and any approved extension period.

Clearly disclose pricing schemes, quantities and dependencies and any restrictions on transfer or reassignment to the BMA.

Development Standards and Methodology

Any configuration, customization, integration or software development must follow controlled engineering and quality management practices.

Methodology

Use a documented development and implementation methodology suitable for a mission-critical government system.

Apply version control, configuration management, peer review and controlled promotion between environments.

Maintain traceability from requirement to design, build, test and acceptance.

Secure development

Embed secure coding standards and automated/static and dynamic security analysis in the development lifecycle.

Resolve security findings rated Medium and above before code check-in or release unless an approved exception applies.

Prevent hidden, malicious or unsupported code from entering the production environment.

Quality management

Maintain a quality management plan describing standards, responsibilities, defect control, review gates and continuous improvement.

Testing, Quality Assurance and User Acceptance

The supplier is responsible for proving that the delivered solution meets functional, technical, security and operational requirements before commissioning.

Test planning

Prepare integrated test plans covering unit/component, integration, system, security, migration, failover, performance and operational readiness.

Define test data, expected results, entry/exit criteria, defect severity classification (aligned with the severity levels defined under Issue management section at 4.26 below) and retest procedures.

Supplier testing

Complete internal system and integration testing before formal BMA acceptance activities.

Provide test evidence and unresolved defect lists.

Ensure production-like test environments are configured sufficiently to validate the solution.

User Acceptance Testing

Support BMA-led UAT, including scripts, data, environment, defect correction and retesting.

Obtain formal approval before cutover.

Acceptance

No material unresolved defect may remain where it affects security, legal compliance, critical operations or agreed performance.

Performance, Load, Stress and Resilience Testing

Performance validation must demonstrate that the platform can support normal, peak and abnormal operating conditions while meeting critical transaction times.

Performance testing

Validate response times for iAPI, search, reporting and integration processes.

Measure application, database, network and infrastructure utilization and identify bottlenecks.

Load testing

Simulate realistic peak and sustained passenger transaction volumes, concurrent users and carrier message patterns.

Confirm capacity assumptions and operational headroom.

Stress and failover testing

Test behavior above expected peaks and during component failure or degraded dependencies.

Verify recovery, transaction integrity, queue handling and failover behavior.

Demonstrate that the system returns to stable operation after stress conditions.

Results

Provide test reports, baseline metrics, exceptions, tuning actions and final approved performance thresholds.

Project Organization and Governance

The project must be governed through a clear structure that enables timely decisions, accountability, escalation and coordination across the BMA, supplier, carriers and third parties.

Supplier organization

Provide an accountable executive sponsor, project manager and suitably qualified technical/workstream leads.

Maintain adequate local and specialist resources throughout implementation and support.

Manage subcontractors as part of the supplier's single point of accountability.

Key personnel

Identify key personnel and obtain approval for material replacements.

Ensure replacement resources have equivalent or better capability and do not reduce service quality.

Project Management, Planning and Progress Reporting

Implementation must be managed through an approved integrated project plan that provides visibility of progress, risks, dependencies and readiness.

Project Management Plan

Define scope, work breakdown, milestones, resources, dependencies, risks, quality controls, communications and acceptance points.

Include carrier onboarding, infrastructure, integration, migration, testing, training, cutover and transition to support.

Progress reporting

Provide regular progress reports (weekly during intensive delivery phases, bi-weekly or monthly thereafter as agreed) covering completed work, planned work, milestone status, risks/issues, decisions, dependencies and actions.

Maintain Risk, Assumption, Issues and Dependencies(RAID)logs and escalate material threats to delivery or service within agreed escalation timelines.

Schedule control

Establish a baseline schedule and manage changes through formal approval.

Track critical path activities and recovery actions where milestones are threatened.

4.21.4. Resource Management

Ensure availability of sufficient human resource capacity thought the contract cycle.

Documentation and Configuration Management

Complete and current documentation is a contractual deliverable and must support BMA operations, audit, training, maintenance and future change.

Required documentation

Application system documentation, solution and security architecture, interface specifications and data models.

System software, hardware and configuration documentation.

Administration/operations manuals, backup/recovery and DR procedures, monitoring and security operations procedures.

User and training guides, test artefacts, migration records and performance reports.

Configuration management

Identify and version-controlled configuration items.

Maintain approved baselines and record changes to software, infrastructure, rules, interfaces and documentation.

Ensure documentation is updated as part of each approved change.

Ownership and format

Provide documentation in BMA-approved editable and final formats.

Transfer all required operational knowledge and artefacts to the BMA at agreed milestones and contract end.

Training, Knowledge Transfer and Change Readiness

The supplier must ensure BMA users, administrators and support personnel are competent to use, govern and support the solution.

Training scope

Role-based training for operational users, supervisors, administrators, security staff and technical support personnel.

Training on passenger processing, risk/targeting, enquiry/reporting, administration, security, monitoring and recovery as relevant.

Training plan

Define audience, prerequisites, objectives, duration, venue/mode, timetable, trainers and assessment method.

Provide BMA-approved training materials and user guides.

Offer refresher or update training when significant changes are introduced.

Knowledge transfer

Use hands-on knowledge transfer during design, testing, cutover and early-life support.

Provide sufficient transfer to reduce avoidable dependency on individual supplier personnel.

System Cutover and Operational Readiness

Production cutover must be planned and executed in a controlled manner that protects border operations, data integrity and service continuity.

Cutover plan

Define sequencing, responsibilities, prerequisites, data migration/final sync, interface activation, validation, communication and rollback criteria.

Include BMA, carrier and third-party readiness checkpoints.

Document decision points and authority for go/no-go.

Pre-cutover readiness

Confirm infrastructure, security acceptance, interfaces, data, operational procedures, support staffing, training and UAT are complete.

Resolve critical defects and obtain formal approvals.

Execution and stabilization

Provide command-center/war-room coordination for go-live.

Monitor transaction processing, interfaces, security and user issues intensively during the stabilization period.

Maintain a tested fallback/rollback approach where technically feasible.

Support and Maintenance — Service Model

The supplier must provide comprehensive operational support for the full solution after commissioning.

Support coverage

Provide 24/7/365 support for production services.

Operate a service desk / support channel capable of receiving, tracking, escalating and reporting incidents and requests.

Provide locally accessible expertise and escalation to product/vendor specialists.

Maintenance

Perform preventive, corrective and adaptive maintenance across hardware, software, integrations, databases, network and security components.

Maintain supported software versions and deploy tested patches and updates.

Coordinate maintenance to minimize service interruption.

Managed operations

Monitor applications, infrastructure, databases, storage, links and security services.

Perform routine administration, health checks, backup/recovery activities and operational reporting.

Issue Management, Severity and Service Levels

A formal issue management process must ensure incidents are recorded, prioritized, escalated and resolved according to business impact.

Issue management system

Provide or use an agreed tool to log, classify, assign, track, escalate and close incidents/problems.

Record symptoms, affected services, actions, root cause, workaround, resolution and closure evidence.

Severity classification

Severity classifications shall be as follows:

a) Severity 1 (Critical): complete loss of a critical border-processing function, a major security breach, or an event with immediate national-security impact.
b) Severity 2 (High): significant degradation of a critical function or a material operational impact requiring urgent restoration.
c) Severity 3 (Medium): partial degradation or impact on a non-critical function where a workable alternative is available.
d) Severity 4 (Low): a minor defect, service request or cosmetic issue with limited operational impact.

The supplier shall apply a severity matrix approved by the BMA before service commencement. The matrix must distinguish Critical, High, Medium and Low incidents according to operational impact, affected scope, security implications and the availability of a workaround.

Treat outages or events with major border/security impact as the highest priority.

Response and updates

Meet BMA-approved response, restoration and resolution targets for each severity (to be formalized in the Service Level Agreement).

Provide frequent updates for critical and high Severity incidents and maintain escalation to senior supplier and OEM resources.

Problem management

Perform root-cause analysis for major/repeat incidents and implement preventive actions.

Service Requests, Change Control and Enhancement Management

The solution must support controlled service requests and software/infrastructure changes without compromising security, stability or traceability.

Service requests

Record, assess, estimate and track operational requests, configuration changes and approved enhancements.

Classify requests by type, urgency, risk and effort.

Change control

No production change may be implemented without BMA-approved change control.

Assess impact on security, integrations, data, performance, documentation, training and rollback.

Test changes in an appropriate non-production environment before release.

Completion criteria

Update relevant documentation and configuration records.

Obtain required test/acceptance evidence and approvals.

Confirm post-implementation verification and close the change only after successful validation.

Key Deliverables and Milestones

The supplier shall deliver a complete set of technical, project, operational and assurance artefacts. Final dates will be agreed in the approved implementation plan, but the minimum milestone structure should remain visible and measurable.

Indicative milestone groups

i) Mobilization and approved project/governance plan.
ii) Approved functional and technical requirements confirmation and solution architecture.
iii) Infrastructure/cloud/DR environments established and secured.
iv) Carrier onboarding and interface implementation.
v) Configured iAPI/PNR, risk engine and targeting, reporting and administration functions.
vi) Data migration and reconciliation completed.
vii) Change-management and operational-readiness documentation.
viii) Security, system, integration, performance and UAT acceptance.

ix) Training and operational readiness completed.
x) Production cutover and stabilization.
xi) Transition to 24/7 managed support and periodic technology refresh.

Core deliverables

Architecture and design packs; project plans; interface documents; functional and technical specifications; user access control modules; migration plan/results; test plans/results; security assurance; training material; cutover plan; operational manuals; SLA/service reports; DR reports; asset/license registers.

Roles and Responsibilities — BMA and Supplier

Successful implementation requires a clear allocation of responsibilities while preserving the supplier's end-to-end accountability for its scope.

BMA responsibilities

Provide governance, business decisions, policy direction and approvals.

Facilitate access to BMA stakeholders, existing environments and relevant information subject to security controls.

Participate in requirements confirmation, UAT, training, readiness and acceptance.

Approve business rules, retention policies, security exceptions, go-live and material changes.

The BMA will establish governance structures, and the service will be expected to form part of those structures.

Supplier responsibilities

Design, supply, implement, integrate, test, secure, document, train, cut over, support and maintain the complete solution.

Coordinate carriers, OEMs, cloud providers and subcontractors within the supplier scope.

Maintain security clearances, skilled personnel, licenses, tooling and service capacity.

Report risks, issues, security events, performance and SLA results.

Supplier accountability

The supplier shall deliver a complete, usable system rather than a set of disconnected products.

The supplier is responsible for all required third-party software, licenses, interfaces, professional services and subcontractor coordination.

The supplier shall provide a fixed implementation schedule and manage delivery through to acceptance and ongoing service

Shared responsibilities

Detailed planning, interface coordination, test scheduling, stakeholder communication and operational transition.

Compliance, Acceptance and Contractual Governance

The solution must operate within South African legal requirements, BMA governance and applicable international passenger data standards.

Legal and regulatory

Comply with the Protection of Personal Information Act, 2013 and other applicable South African legal and regulatory obligations.

Comply with ICAO Annex 9 passenger data exchange requirements and ICAO Doc 9944 guidance applicable to PNR.

Use BMA-approved information classification, handling, retention and security requirements.

Security and personnel

Ensure personnel and subcontractors hold required security clearance before accessing the system or classified information.

Protect classified information during the contract and securely return, erase or destroy it at contract end as directed.

Acceptance governance

The BMA may reject components or the solution where material security, performance or acceptance requirements remain unmet.

Any waiver or deviation requires formal BMA approval supported by justification and risk assessment.

Audit, reporting and remediation obligations continue throughout the contract.

Bidder Response Framework and High-Level Compliance Schedule

Bidders should structure proposals so that the BMA can clearly determine compliance, capability, delivery risk and total solution accountability. Responses should distinguish between compliance statements and explanatory evidence rather than merely repeating the TOR wording.

Required proposal structure

Executive summary and understanding of BMA objectives.

End-to-end solution description and architecture.

Functional capability response: PNR, iAPI, manifests, risk/targeting, search/reporting, data management.

Technical/non-functional response: hosting, DR, performance, security, integration, software/hardware.

Implementation, carrier onboarding, migration, testing, training and cutover approach.

Project organization, local capability and key personnel.

24/7 support, SLA, issue management, service requests and technology refresh.

Compliance, licenses, certifications, references and assumptions.

Detailed pricing aligned to mandatory and optional requirements.

Closing requirement

The successful bidder will be expected to refine the high-level TOR into approved detailed designs, implementation artefacts, operating procedures and acceptance baselines without reducing the mandatory outcomes defined herein.

General and Other Requirements

Preference may be given, in accordance with the published evaluation criteria, to service providers that demonstrate relevant experience in law-enforcement, border-management,

customs, immigration or other security-sensitive government environments.

The service provider should demonstrate experience in implementing and supporting passenger-processing, integration and ICT infrastructure across Ports of Entry, airports, seaports and other geographically dispersed operational environments.

CONFIDENTIALITY OF INFORMATION

All information shared during this bidding process and, if the supplier is appointed, during implementation and operation remains the property of the BMA. It must be kept in strict confidence and may not be used or disclosed for any purpose other than the performance of the contract, unless authorised in writing by the BMA.

PAYMENT

The supplier will be paid in South African Rand at a fixed price, inclusive of VAT, for services rendered.

Payment will be made within 30 days after receipt and approval of a valid invoice, in accordance with the agreed payment schedule.

Payment will be linked to the approved deliverables and milestones set out in this TOR, subject to achievement of the required professional and service-level standards. Any dispute concerning performance standards will be managed in accordance with the dispute-resolution provisions of the contract.

RULES OF BIDDING AND RFP SUBMISSION REQUIREMENTS

The Border Management Authority reserves for itself the right to only appoint and enter into a contractual agreement with one entity or multiple entities for the services required, 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.

The Border Management Authority reserves the right to terminate this appointment or temporarily defer the work, or any part thereof, should it deem necessary. Should the contract 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.

No data obtained, generated or processed in performing the contract may be used for any other purpose without the BMA's prior written authorization.

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.

THE BIDS WILL BE EVALUATED AS FOLLOWS

Stage 1 Administrative Compliance

Bidders must ensure that the following documents are completed, signed where required and submitted with the bid:

(i) SBD 1: Invitation to quote/bid

(ii) SBD 3: Pricing Schedule

(iii) SBD 4 form: Bidders Disclosure

(iv) Authority to sign the bid

(v) SBD 6.1 form: Preference Points Claim Form in terms of the Preferential Procurement Regulations, 2022. Tenderers must indicate the specific goals for which points are claimed and submit the prescribed supporting evidence. (Attach active BBBEE certificate or Affidavit)

(vi) SBD 7:Contract Form

Only bidders that meet the Stage 1 requirements will be evaluated at Stage 2.

Stage 2 Mandatory Requirements

Bidders must meet every mandatory requirement on a pass/fail basis. The BMA reserves the right to verify all information and supporting evidence provided.

Only bidders that meet every mandatory requirement will proceed to Stage 3

No.	Mandatory requirements	Evidence of compliance
1	The bidder must accept full accountability for the iAPI, PNR, passenger risk engine, targeting capability, carrier gateway, private-cloud infrastructure and all subcontractors.	The bidder must attach a Signed undertaking form/letter accepting end-to-end accountability.
2	Demonstrate experience of at least three (3) national or multi-jurisdictional government or government entities implementations that processed per-passenger iAPI and returned boarding directives to carrier departure control systems.	The bidder must attach three (3) client reference letters, signed, , on the client's letterhead and stating the scope, and implementation period. The BMA reserves the right to verify the information provided and may request referee contact details from shortlisted bidders.
3	Demonstrate experience of at least three (3) government or government entities implementations that acquired and processed PNR information for passenger risk assessment using recognised PNR reporting standards.	The bidder must attach three (3) signed client references letters, in the client's letterhead, stating the description, scope of work and implementation period. The BMA reserves the right to verify the information provided and may request referee contact details from shortlisted bidders.
4	Existing or contractually secured capability to connect, certify and support multiple international carriers and different reservation or departure control systems.	Attach OEM certificate confirming the carrier-gateway capability. OR Where the bidder is not the OEM, an OEM certificate confirming the required carrier-gateway capability, together with a valid agreement or authorisation letter or equivalent binding contractual evidence between the bidder and the OEM confirming that the bidder is authorised and has secured access to the capability required to deliver the contract must be attached

5	The bidder must demonstrate ownership of the proposed core software or hold valid authority to supply, configure, support and maintain it for the full term.	Attach OEM ownership letter where the bidder is the OEM declaring that you can supply, implement and support the proposed product for the contract term or where the bidder is not the OEM; provide a OEM ownership letter together with valid agreement or authorisation letter or equivalent binding contractual evidence between the bidder and OEM authorising the bidder to supply, implement and support the proposed product for the contract term must attached.
6	The proposed solution must support PAXLST, PNRGOV and applicable EDIFACT or XML message exchange including interactive response messaging.	A signed declaration by the bidder confirming that the proposed solution supports PAXLST, PNRGOV and the applicable EDIFACT formats and XML schemes specified in the TOR must be submitted.
7	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 OEM/OSM bidding, only submit the OEM/OSM certificate.

Stage 3 Live Demonstration

Bidders will be required to perform a live, scripted demonstration using the proposed product or a current representative production release. Slides, static screenshots, recordings and custom mock-ups will not be accepted as substitutes. Bidders are expected to conduct a live demonstration using a virtual platform.

Demonstration factor	Required scenario	Scoring methodology	Weight
Carrier message ingestion and validation	Receive valid and malformed API and PNR messages and show validation, acknowledgement, duplicate handling, traceability, exception handling and monitoring.	Scenario not demonstrated or required outcome not achieved = 0 Scenario demonstrated and required outcome achieved = 15	15
Interactive check-in decision	Process an iAPI transaction, perform the approved checks and return a Board or No Board directive with latency, reasons, delivery evidence and an audit trail.	Scenario not demonstrated or required outcome not achieved = 0 Scenario demonstrated and required outcome achieved = 15	15
PNR lifecycle and reconciliation	Ingest successive PNR updates and reconcile them with API, boarding and final-manifest data while preserving history and discrepancies.	Scenario not demonstrated or required outcome not achieved = 0 Scenario demonstrated and required outcome achieved = 10	10
Watchlist and identity matching	Demonstrate exact and fuzzy matching, threshold control, false-positive handling and alert evidence using a synthetic watchlist.	Scenario not demonstrated or required outcome not achieved = 0 Scenario demonstrated and required outcome achieved = 10	10

Demonstration factor	Required scenario	Scoring methodology	Weight
Passenger risk-rule lifecycle	Create a multi-factor rule without code; simulate, peer-review, approve, version and deploy it; and generate a risk alert.	Scenario not demonstrated or required outcome not achieved = 0 Create a multi-factor rule without code; simulate, peer-review, approve, version and deploy it = 10 Scenario demonstrated and required outcome achieved = 15	15
Analyst workflow and link analysis	Triage, assign and escalate an alert; show related travellers, bookings, documents or contacts; and record the disposition and outcome.	Scenario not demonstrated or required outcome not achieved = 0 Scenario demonstrated and required outcome achieved = 10	10
Search, reporting and audit	Perform a multi-parameter enquiry, generate a report, export an authorised result and show user. Inclusion of decision audit records and trails.	Scenario not demonstrated or required outcome not achieved = 0 Perform a multi-parameter enquiry, generate a report, export an authorized result and show user. = 5 Scenario fully demonstrated and all required outcome achieved = 10	10

Demonstration factor	Required scenario	Scoring methodology	Weight
Administration, security and segregation	Show role-based access, masking, privileged-action control, session security and separation between rule author and approver.	Scenario not demonstrated or required outcome not achieved = 0 Scenario demonstrated and required outcome achieved = 5	5
Private-cloud infrastructure and recovery readiness	Demonstrated private cloud is capable of using scalable ICT server infrastructure, show capacity and health monitoring, backup and replication status. With additions of security controls, recovery orchestration and evidence of a successful recovery or failover test.	Scenario not demonstrated or required outcome not achieved = 0 Demonstrated private cloud is capable of using scalable ICT server infrastructure, show capacity and health monitoring, backup and replication status. = 5 Scenario fully demonstrated and all required outcome achieved = 10	10

The live demonstration is scored out of 100 points. A bidder must achieve **at least 75 points** overall to proceed to Stage 4. Failure to demonstrate any scenario will result in a score of zero for that scenario.

Stage 4 Price and Specific Goals Evaluation

Preferential Procurement Evaluation Based On The 90/10 Principle

The applicable formula (90/10) will be utilised to evaluate the bid, of which ninety (90) points are allocated for price as allocated in the enclosed form SBD 6.1. that must be completed, and the remaining ten (10) points are allocated for the specific goals as indicated in the table below
Responsive bids will be adjudicated by the State on the 90/10-preference point claim in terms of the Preferential Procurement Regulation 2022 which points are awarded to bidders on the basis of:
The bid price (maximum 90 points)

Specific Goals (maximum 10 points)