

INVITATION TO BID

BID NO:

RAF/2026/00059

BID DESCRIPTION:

**PROCUREMENT OF A THREAT DETECTION AND RESPONSE SERVICES FOR THE ROAD
ACCIDENT FUND (RAF) FOR A PERIOD OF FIVE (5) YEARS.**

PUBLICATION DATE: 10 SEPTEMBER 2026

NON-COMPULSORY BRIEFING SESSION DATE AND TIME: 22 SEPTEMBER 2026

@ 11:00 AM

A NON-COMPULSORY BRIEFING SESSION WILL BE HELD ON TEAMS:

<https://teams.microsoft.com/meet/351818207347668?p=8tu6wsXapZXCYCYNSL>

CLOSING DATE: 09 OCTOBER 2026 @ 11H00 AM

***Note: Faxed and/or Emailed Proposals/ bids will not be accepted, only hand delivered and
couriered Proposals/ bids must be deposited in the tender box on or before the closing date and
time.***

TABLE OF CONTENTS FOR BID RAF/2026/00059

1. PART A: INVITATION TO BID
2. PART B: TERMS AND CONDITIONS FOR BIDDING
3. SBD 3.3: PRICING SCHEDULE (PROFESSIONAL SERVICES)
4. SBD 4: DECLARATION OF INTEREST
5. SBD 5: NATIONAL INDUSTRIAL PARTICIPATION PROGRAMME
6. SBD 6.1: PREFERENCE POINTS CLAIM FORM
7. SPECIFICATION DOCUMENT
8. GENERAL CONDITIONS OF CONTRACT

IMPORTANT NOTES:

1. Bid documents are available on the website (www.raf.co.za) at no cost.

2. Submission of Proposals

- Bid responses must be placed in the tender box clearly marked with a tender number and description; and
- Bidders are required to submit an original Bid Document/Proposal and a Copy (To be enclosed in the envelope which contains the Original Bid Document/Proposal)
- The proposal must be deposited in the tender box situated at the reception of RAF at the address given below:

**Road Accident Fund (RAF), Eco Glades 2 Office Park, 420 Witch-hazel Avenue,
Centurion, 0046**

3. Validity Period

The proposal submitted by the supplier must be valid for a period of 90 days, from the closing date for the submission of proposals.

4. Enquiries

All enquiries regarding this bid must be directed to the Supply Chain Management Office:

Bid Enquiries: Tshiamo Motitswe

E-mail address: Tshiamomo@raf.co.za.

Note: No telephonic enquiries will be entertained.

Closing date and time for Bid questions and enquiries: **25 September 2026**

Publication date for Questions & Answers: **30 September 2026**

Questions and Answers will be published on the RAF website and eTender portal.

Important Notes:

1. All questions/enquiries must be forwarded in writing to the e-mail address above; and
2. Questions/enquiries received after the above-stated date and time will not be entertained.

LEGISLATIVE REQUIREMENTS

This stage checks and validates the bidders' compliance to the legal requirements to conduct business in South Africa, as well as to the industry requirement for the supply of goods and services.

Returnable Documents / Information	Check list ✓ Tick each box
SBD 1: Completed, attached and signed	
SBD 3.1 or 3.2 or 3.3 Completed, attached and signed	
SBD 4: Completed, attached and signed	
SBD 5: Completed, attached and signed	
SBD 6.1: Completed, attached and signed	
Proof of Construction Industry Development Board (CIDB) registration, if applicable.	
Specification document	
General Condition of contract	
Provide Tax TCS Pin to verify Tax Status: Attached (In bids where Consortia/Joint Ventures/Sub-contractors are involved, each party must submit a separate Tax TCS Pin.)	
If the bidder is a joint venture, consortium or other unincorporated grouping of two or more persons/ entities, a copy of the joint venture agreement between the members should be provided.	
Registered on the Central Supplier Database of National Treasury. (For registration information, go to https://secure.csd.gov.za/)	

Note: Some requirements may not be applicable to international suppliers/ bidders and only those suppliers/ bidders will be exempted from these mandatory/ legislative requirements. All SBDs must be submitted (signed) noting where it is not applicable.

PART A INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE ROAD ACCIDENT FUND					
BID NUMBER:	RAF/2026/00059	CLOSING DATE:	09 OCTOBER 2026	CLOSING TIME:	11H00
DESCRIPTION	PROCUREMENT OF A THREAT DETECTION AND RESPONSE SERVICES FOR THE RAF FOR A PERIOD OF FIVE (5) YEARS.				
BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT:					
ROAD ACCIDENT FUND (RAF) ECO GLADES 2 OFFICE PARK					
420 WITCH-HAZEL AVENUE					
CENTURION					
0046					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO			TECHNICAL ENQUIRIES MAY BE DIRECTED TO:		
CONTACT PERSON	Tshiamo Motitswe		CONTACT PERSON		
TELEPHONE NUMBER			TELEPHONE NUMBER		
FACSIMILE NUMBER	N/A		FACSIMILE NUMBER		
E-MAIL ADDRESS	Tshiamomo@raf.co.za		E-MAIL ADDRESS		
SUPPLIER INFORMATION					
NAME OF BIDDER					
POSTAL ADDRESS					
STREET ADDRESS					
TELEPHONE NUMBER	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

1 ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	☐ Yes ☐ No [IF YES ENCLOSE PROOF]	2 ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES /WORKS OFFERED?	☐ Yes ☐ No [IF YES, ANSWER THE QUESTIONNAIRE BELOW]
--	--	---	---

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.	

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 PIN 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)

PRICING SCHEDULE – FIRM PRICES**(PURCHASES)**

NOTE: ONLY FIRM PRICES WILL BE ACCEPTED. NON-FIRM PRICES (INCLUDING PRICES SUBJECT TO RATES OF EXCHANGE VARIATIONS) WILL NOT BE CONSIDERED

IN CASES WHERE DIFFERENT DELIVERY POINTS INFLUENCE THE PRICING, A SEPARATE PRICING SCHEDULE MUST BE SUBMITTED FOR EACH DELIVERY POINT

Name of bidder.....	Bid number.....
Closing Time 11:00	Closing date.....

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

ITEM NO.	QUANTITY	DESCRIPTION	BID PRICE IN RSA CURRENCY ** (ALL APPLICABLE TAXES INCLUDED)
----------	----------	-------------	---

-
- Required by:
 - At:
.....
 - Brand and model
 - Country of origin
 - Does the offer comply with the specification(s)? *YES/NO
 - If not to specification, indicate deviation(s)
 - Period required for delivery
*Delivery: Firm/not firm
 - Delivery basis

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

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

*Delete if not applicable

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

- 1.1 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, 1996 (Constitution), and further expressed in the various applicable legislation, it is required for the bidder to make this declaration in respect of the details required hereunder.
- 1.2 If a person is 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. DECLARATION ON EMPLOYMENT BY ORGAN OF STATE

- 2.1 Is the bidder, or any of the directors / trustees / shareholders / members / partners of the bidder employed by an organ of state, as defined in section 239 of the Constitution?
YES/NO
- 2.2 If YES, furnish particulars of the names, individual identity numbers, in the table below:

Full Name	Identity Number	Name of organ of state

- 2.3 Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution? **YES/NO**

ⁱ 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.

2.3.1 If so, furnish particulars:

.....
.....
.....

2.4 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**

2.4.1 If so, indicate all companies registered in the CSD in the table below:

Supplier registration number (MAAA)	Status (active/inactive/deleted)

Failure to disclose all CSD-registered active companies linked to all Directors will lead to disqualification.

3 GENERAL DECLARATION

I,, the undersigned, 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 to be false.
- 3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor.
- 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.
- 3.5 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.
- 3.6 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.

3.7 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act, 1998 (Act No. 89 of 1998) and or may be referred to law enforcement agencies for criminal investigation and or may be restricted from conducting business with the state for a period not exceeding 10 years in terms of the Prevention and Combating of Corrupt Activities Act, 2004 (Act No. 12 of 2004) or any other applicable legislation.

I CERTIFY THAT THE ABOVE IS CORRECT.

I ACCEPT THAT THE PROCURING INSTITUTION MAY REJECT THE BID OR TAKE APPROPRIATE ACTION AGAINST ME IF THIS DECLARATION IS FALSE.

.....

Signature

.....

Date

.....

Designation

.....

Name of bidder

THE NATIONAL INDUSTRIAL PARTICIPATION PROGRAMME INTRODUCTION

The National Industrial Participation (NIP) Programme, which is applicable to all government procurement contracts that have an imported content, became effective on 1 September 1996

The NIP Policy and Guidelines were fully endorsed by Cabinet on 30 April 1997. In terms of the Cabinet decision, all state and parastatal purchases/lease contracts for (for goods, works and services) entered into after this date, are subject to the NIP requirements. NIP is obligatory and therefore must be complied with. The Industrial Participation Secretariat (IPS) of the Department of Trade and Industry (dti) is charged with responsibility of administering:

1. PILLARS OF THE PROGRAMME

- 1.1 The NIP obligation is benchmarked against the imported content of the contract. Any Contract having an imported content equal to or exceeding US\$10 million or other currency equivalent to US\$10 million will have an NIP obligation. This threshold of US\$10 million can be reached as follows:

(a) Any single contract with imported content exceeding US\$10 million.

Or

(b) Multiple contracts for the same goods, works or services each with imported content exceeding US\$3 million awarded to one seller over a two-year period which exceeds US\$10 million in total.

Or

(b) A contract with a renewable option clause, where should the option be exercised, the total value of the imported content will exceed US\$10 million.

Or

(d) Multiple suppliers of the same goods, works or services under the same contract, where the value of the imported content of each allocation is equal to or exceeds US\$3 million worth of goods, works or services to the same government institution, which in total over a two-year period exceeds US\$10 million.

- 1.2 The NIP obligation applicable to suppliers in respect of subparagraphs 1.1 (a) to 1.1 (c) above will amount to 30% of the imported content, whilst suppliers in respect of sub-paragraph 1.1 (d) shall incur 30% of the total NIP obligation on a pro-rata basis.
- 1.3 To satisfy the NIP obligation, the dti would negotiate and conclude agreements such as investments, joint ventures, sub-contracting, license production, export promotion, sourcing arrangements and reaseracg and development (R&D) with partners, or suppliers
- 1.4 A period of seven years has been identified as the time frame within which to discharge the obligation.

2. REQUIREMENTS OF THE DEPARTMENT OF TRADE AND INDUSTRY

- 2.1 In order to ensure effective implementation of the programme, successful bidders (contractors) are required to, immediately after the award of the contract.

that is in excess of R10 million, submit details of such a contract to the dti for reporting purposes.

- 2.2 The purpose for reporting details of contracts in excess of the amount of R10 million is to cater for multiple contracts for the same goods, works, services; renewable contracts and multiple suppliers for the same goods, works or services under the same contract as provided for in sub-paragraphs 1.1 . (b) to 1.1. (d) above.

3. BID SUBMISSION AND CONTRACT REPORTING REQUIREMENTS OF THE BIDDERS AND SUCCESSFUL BIDDERS (CONTRACTS)

- 3.1 Bidders are required to sign and submit this Standard Bidding Document (SBD 5) together with the bid on the closing date and time.

- 3.2 In order to accommodate multiple contracts for the same goods, works or services, renewable contracts and multiple suppliers for the same goods, works or services under the same contract as indicated in sub-paragraphs 1.1 (b) to 1.1 (d) above and to enable the dti in determining the NIP obligation , successful bidders (contractors) are required, immediately after being officially notified about any successful bid with a value in excess of R10 million, to contact and furnish the dti with the following information:

- Bid/contract number;
- Description of the goods, works or services;
- Date on which the contract was accepted;
- Name, address and contact details of the government institution;
- Value of the contract; and
- Imported content of the contract, if possible.

- 3.3 The information required in paragraph 3.2 above must be sent to the Department of Trade and Industry, Private Bag X 84, Pretoria, 0001 for the attention of Mr Elias Malapane within five (5) working days after the award of the contract. Mr Malapane may be contacted on the telephone number (012) 394 1401, facsimile (012) 394 2401 or e-mail at Elias@thedti.gov.za for further details about the programme.

4 PROCESS TO SATISFY THE NIP OBLIGATION

- 4.1 Once the successful bidder (contractor) has made contact with and furnished the dti with the information required, the following steps will be followed:

- a. The contractor and the dti will determine the NIP obligation;
- b. The contractor and the dti will sign the NIP obligation agreement;
- c. The contractor will submit a performance guarantee to the dti;
- d. The contractor will submit a business concept for consideration and approval by the dti;
- e. Upon approval of the business concept by the dti, the contractor will submit

- detailed business plans outlining the business concepts;
- f. The contractor will implement the business plans; and
 - g. The contractor will submit bi-annual progress reports on approved plans to the dti.

4.2 The NIP obligation agreement is between the dti and the successful bidder (contractor) and, therefore, does not involve the purchasing institution.

Bid number	
Closing date:	
Name of bidder:	
Postal address	
.....	
.....	
Signature.....	Name (in print).....
Date.....	

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**

(delete whichever is not applicable for this tender).

a) The applicable preference point system for this tender is the 80/20 or 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	POINTS
PRICE	80	90
SPECIFIC GOALS	20	10
Total points for Price and SPECIFIC GOALS	100	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:

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \mathbf{Ps} = \mathbf{80} \left(\mathbf{1} - \frac{\mathbf{Pt} - \mathbf{Pmin}}{\mathbf{Pmin}} \right) & \mathbf{or} & \mathbf{Ps} = \mathbf{90} \left(\mathbf{1} - \frac{\mathbf{Pt} - \mathbf{Pmin}}{\mathbf{Pmin}} \right) \end{array}$$

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:

$$\begin{array}{ccc} \mathbf{80/20} & \mathbf{or} & \mathbf{90/10} \\ \mathbf{Ps} = \mathbf{80} \left(\mathbf{1} + \frac{\mathbf{Pt} - \mathbf{Pmax}}{\mathbf{Pmax}} \right) & \mathbf{or} & \mathbf{Ps} = \mathbf{90} \left(\mathbf{1} + \frac{\mathbf{Pt} - \mathbf{Pmax}}{\mathbf{Pmax}} \right) \end{array}$$

Where

- Ps = Points scored for price of tender under consideration
 Pt = Price of tender under consideration
 Pmax = Price of highest acceptable tender

4. POINTS AWARDED FOR SPECIFIC GOALS

- 4.1. In terms of Regulation 4(2); 5(2); 6(2) and 7(2) of the Preferential Procurement Regulations, preference points must be awarded for specific goals stated in the tender. For the purposes of this tender the tenderer will be allocated points based on the goals stated in table 1 below as may be supported by proof/ documentation stated in the conditions of this tender:
- 4.2. In cases where organs of state intend to use Regulation 3(2) of the Regulations, which states that, if it is unclear whether the 80/20 or 90/10 preference point system applies, an organ of state must, in the tender documents, stipulate in the case of—
- (a) an invitation for tender for income-generating contracts, that either the 80/20 or 90/10 preference point system will apply and that the highest acceptable tender will be used to determine the applicable preference point system; or
 - (b) any other invitation for tender, that either the 80/20 or 90/10 preference point system will apply and that the lowest acceptable tender will be used to determine the applicable preference point system,
- then the organ of state must indicate the points allocated for specific goals for both the 90/10 and 80/20 preference point system.

Table 1: Specific goals for the tender and points claimed are indicated per the table below.

(Note to organs of state: Where either the 90/10 or 80/20 preference point system is applicable, corresponding points must also be indicated as such.)

Note to tenderers: The tenderer must indicate how they claim points for each preference point system.)

The specific goals allocated points in terms of this tender	Number of points allocated (80/20 system) (To be completed by the organ of state)	Number of points allocated (90/10 system) (To be completed by the organ of state)	Number of points allocated (80/20 system) (To be completed by the tenderer)	Number of points claimed (90/10 system) (To be completed by the tenderer)
South African citizen who had no franchise in national elections prior to the introduction of the Constitution of the Republic of South Africa, 1983 (Act 200 of 1983) or the Constitution of the Republic of South Africa, 1996. (minimum 51%	10	5		

ownership or more)				
Women (minimum 51% ownership or more)	8	4		
Persons with disabilities (minimum 51% ownership or more)	2	1		

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:	
	
	
	
	

BID SPECIFICATION – PROCUREMENT OF A THREAT DETECTION AND RESPONSE SERVICES FOR THE RAF FOR A PERIOD OF FIVE (5) YEARS.

1. BACKGROUND OF THE ROAD ACCIDENT FUND

The Road Accident Fund (RAF) is a schedule 3A Public Entity established in terms of the Road Accident Fund Act, 1996 (Act No. 56 of 1996), as amended. Its mandate is the provision of compulsory social insurance cover to all users of South African roads, to rehabilitate and compensate persons injured as a result of the negligent driving of motor vehicles in a timely and caring manner, and to actively promote the safe use of our roads.

The customer base of the RAF or the Fund comprises not only the South African public, but all foreigners who may have had accidents within the borders of the country. The RAF head office is located in Centurion, Pretoria; with Customer Experience Centres situated in each province around the country.

2. SPECIAL INSTRUCTIONS TO BIDDERS

- 2.1. The bidder/s must be an eligible, registered service provider/s in terms of the applicable laws of the country.
- 2.2. The bidder/s must have a business continuity management plan, which must be available for inspection by the RAF during the subsistence of rendering services to the RAF.
- 2.3. The Evaluation Criteria that are published with this Request for Proposal/ Bids will be used to assess bidders' responses and no amendment shall be made after the closing date of a bid. Bid Proposals must be clearly indexed and cross referenced to a Table of Contents.
- 2.4. Companies or Directors included on the National Treasury register of Restricted Suppliers and/ or Tender Defaulters will be automatically disqualified from the bidding process.
- 2.5. As prescribed all Standard Bidding Documents (SBD Forms – Returnable Documents) must be fully completed and duly signed. All Returnable Documents must be submitted with the proposal on the closing date of the bid.
- 2.6. The RAF will confirm the following prior to any award being made:
 - That the bidder/s is/ are registered on the National Treasury Central Supplier Database (CSD)
 - The bidder's tax status is compliant with the South African Revenue Service (SARS), in cases where the recommended bidder/s is/ are non-compliant with SARS, the bidder/s will be allowed seven (7) working days to rectify their tax matters, if the bidder/s fails to rectify their tax matters, they will be disqualified once the 7th working day period lapses.
- 2.7. The bidder/s shall have Professional Indemnity cover, which must be available prior to the award, which shall extend to include Privacy breach and cyber liability (extension/endorsement).

- 2.8. The service provider/s agrees to indemnify and hold the Fund harmless from and against any claims, losses, damages, or expenses incurred as a result of any breach arising out of or attributable to the Service Provider's negligent acts or omissions.
- 2.9. The Bidder/s must implement or consider the principles of Privacy by Design and Privacy by Default when reviewing, redesigning and recommending business processes.
- 2.10. The Bidder/s must ensure that all information stored electronically is protected through appropriate encryption, authentication, logging and monitoring controls where applicable
- 2.11. The Bidder/s must not transfer, store or process RAF information outside the Republic of South Africa without the RAF's prior written approval and compliance with applicable legal requirements.
- 2.12. The Bidder/s must permit the RAF, or its authorised representatives, to conduct privacy, information security and compliance assessments or audits relating to the processing of RAF information.

3. BACKGROUND OF THE BID

- 3.1. The Road Accident Fund (RAF) seeks to appoint a qualified Service Provider to provide a 24/7/365 Managed Threat Detection and Response (TDR) service, for a period of five (5) years, to monitor, detect, contain, and remediate IT threats across applications, devices, systems, network, and locations.
- 3.2. The service provider will be responsible for the end-to-end monitoring, detection, and response of the RAF's existing in-house Microsoft Sentinel TDR solution and associated detected threats. This entails automated, proactive threat-hunting environment that leverages the RAF's current technology investments.

4. THE SCOPE OF REQUIREMENTS:

- 4.1. The successful bidder must provide 24/7/365 managed TDR services for a period of five (5) years.
- 4.2. The bidder must provide 24/7/365 **Cybersecurity Monitoring & Triage**, which includes:
 - 4.2.1 Continuous monitoring of all security alerts generated by the in-house (RAF-Owned) Microsoft Sentinel TDR.
 - 4.2.2 Initial triage to filter false positives and escalate and resolve "True Positive" incidents.
 - 4.2.3 Contextualised alerting based on RAF's business risk and asset criticality.
 - 4.2.4 Real-time monitoring and threat detection of the RAF's on-premises and cloud-based systems, applications, and infrastructure. All incidents must be promptly identified, escalated, and addressed.
 - 4.2.5 Monitoring the RAF's environment, including cloud services (AWS, Azure, and Oracle cloud) and on-premise for potential security incidents and unauthorized activity.
 - 4.2.6 Log Management: Collection and retention of logs from multiple systems and generate reports that can be used to provide a holistic view of the environment.
 - 4.2.7 **Threat Intelligence Integration:** integration of global threat intelligence feeds to

detect and respond to emerging threats proactively.

4.3. **SIEM Engineering & Data Onboarding**

4.3.1 Full management of the SIEM architecture and platform (excluding licensing costs).

4.3.2 Onboarding of new data sources (Syslog, API, Cloud logs, Agents). These data sources include servers, workstations, applications, network infrastructure and cybersecurity solutions.

4.3.3 Health monitoring of data connectors and log ingestion pipelines to ensure no visibility gaps.

4.4. **Detection Engineering & Tuning**

4.4.1 Continuous optimisation and tuning of detection rules to reduce "alert fatigue."

4.4.2 Mapping of all detection use cases to the **MITRE ATT&CK Framework**.

4.4.3 Custom rule creation based on emerging threats specific to the South African government and financial sectors.

4.4.4 Leveraging open-source detection use cases such as Sigma.

4.5. **Incident Response, Containment and SOAR Automation**

4.5.1 Implementation and management of **SOAR (Security Orchestration, Automation, and Response)** and/or Incident Response (IR) playbooks for containment and eradication to automate repetitive tasks (e.g., blocking IPs, isolating compromised endpoints).

4.5.2 Deep-dive forensic analysis for high-criticality incidents.

4.5.3 **Incident Triage and Analysis:** prompt triage and analyse security incidents in the environment to determine severity, scope, and impact.

4.5.4 **Incident Containment and Remediation:** contain and remediate security incidents in the environment to minimise their impact and duration, including the execution of Incident Response (IR) playbooks for containment and eradication.

4.5.5 **Communication and Coordination:** communicate and coordinate with internal and external stakeholders to resolve security incidents and address security risks.

4.5.6 **Active Response & Lockdown:** In the event of a confirmed breach (like the current stolen access information), the service provider should have the authority to isolate infected machines or lock compromised accounts immediately, through pre-approved TDR actions and operating models.

4.5.7 **Root Cause Analysis (RCA):** Post-incident investigations to determine how the breach occurred and how to harden the system against future occurrences.

4.5.8 **Crisis Management Support:** Access to a dedicated Incident Response team for large-scale events.

4.6 Threat Hunting

4.6.1 **Threat Hunting:** use advanced security technologies and techniques to conduct ongoing threat hunting activities to identify and mitigate potential security threats in the environment.

4.6.2 **Threat Intelligence:** provide ongoing threat intelligence and analysis to inform the RAF's security posture and decision-making processes.

4.6.3 **Manage Threats:** Integrate the RAF's cybersecurity solutions to automate responses to identified threats that pose risks to the RAF environment.

4.7 Threat Response

4.7.1 Design of implementation of manual, semi-automated and automated responses and recovery actions to detected threats and cyberattacks.

4.8 Service Migration (Incumbent Transition)

4.8.1 A structured 30-to-60-day transition plan from the current service provider.

4.8.2 Knowledge transfer, migration of existing custom workbooks/dashboards, and validation of current alerting logic.

4.9 Integration with existing security tools

4.9.1 **Automated data sharing:** the integration should allow for seamless and automated data sharing between the existing security tools and the TDR platform, thus eliminating manual processes and reducing the risk of human error.

4.9.2 **Seamless workflows:** the integration should support seamless workflows between existing security tools and the TDR platform thus reducing the time and effort required to switch between different tools and platforms.

4.9.3 **Centralized management and monitoring:** the integration should allow for centralized management and monitoring of security events, alerts, and incidents, making it easier to track and respond to security incidents.

4.9.4 **Data enrichment:** the integration should allow for the enrichment of data from existing security tools with data from the TDR platform thus providing a more comprehensive and accurate view of security incidents and threats.

4.10 Skills Transfer

The service provider must provide continuous skills transfer to 10 cybersecurity personnel throughout the contract, including during and after implementation. As part of this process, service providers must provide:

4.10.1 Detailed TDR administration, customisation, data source onboarding, integration and incident response playbook manuals

4.10.2 Configuration documentation

4.10.3 SOC escalation procedures and escalation matrix

4.11 SOC Premises

To maintain uptime, the SOC command centre premises must meet the following requirements:

4.11.1 Access Controlled

- Minimum: Fingerprint or Token/Card Access control

4.11.2 Power Failure Backup

- Backup Power restored within a minute
- Business Continuity Plan

4.11.3 Fire Detection System

- Certificate of compliance for the fire detection system.
- Certificate of service should not be older than 1 year from the date of the site visit.

4.12 SOC Personnel

4.12.1 The service provider is required to have an SOC Team that has the right skills, using the least number of resources. The SOC Team should have at least a three tiers level of support (Tier 1, Tier 2 and Tier 3) for escalations and reporting.

4.12.2 The following dedicated personnel are required as part of the requested service:

- 1 x SOC service delivery manager
- 1 x SOC threat management lead as a central technical point of contact

4.13 Service Level Agreements and Reporting

- Service Level Agreements (SLAs): the SLAs must be aligned with the RAF's requirements and expectations and must be reviewed and updated regularly to ensure that they remain relevant and effective.
 - The service provider must respond to and resolve all calls for incidents logged within the following time frames (service levels):

Category	Response	Resolution
Priority 1 – Urgent	15 minutes	1 hour
Priority 2 – High	30 minutes	2 hours
Priority 3 – Medium	45 minutes	6 hours
Priority 4 – Low	60 minutes	+10 hours

- **Reporting:** the service provider must provide regular reports to the RAF that provide insight into the performance and effectiveness of its services. The reports must be easy to understand and provide information such as the number of security incidents detected, the number of security incidents resolved, and the time taken to resolve them.
- **Metrics:** the SOC must have a set of metrics in place that measure the performance and effectiveness of its services, including Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). The metrics must align with the SLAs and be used to track and report on the SOC's performance.
- **Performance Management:** the SOC must have a performance management process in place that assesses the performance of its services regularly and identifies areas for improvement. The performance management process must be based on the metrics and SLAs and must be used to identify and prioritise areas for improvement.
- **CISO Dashboards:** Real-time visibility into the organisation's risk score and the status of remediation actions.
- **Continuous Improvement:** The SOC must be capable of adapting to the new industry standards.
- **Post-Incident Review and Reporting:** conduct a post-incident review and provide detailed reporting on the incident and outcome to relevant stakeholders.

4.14 SOC Operating Model

The TDR Service should operate and function on the following key aspects which are the basics of forming an effective SOC:

- 4.13.1 **People (SOC Team):** competent and qualified SOC Team to monitor, prevent, detect, investigate, and respond to all cyber threats.
- 4.13.2 **Processes:** establish a key process to build an effective SOC; these include event classification and triage; prioritization and analysis; remediation, recovery and assessment, audit, etc.
- 4.13.3 **Technology:** review the essential security monitoring tools for building an SOC including Asset Discovery, Vulnerability Assessment, Intrusion Detection, Behavioural Monitoring, Security Information and Event Management (SIEM), etc.
- 4.13.4 **Intelligence:** understand the differences among tactical, strategic, and operational intelligence and the specific ways these are used within the SOC-as-a-Service⁵

4.15 Business Requirements:

4.15.1 Service Requirements

For ease of evaluation, bidders are required to provide a clear cross-reference to relevant section(s) of their proposal addressing each requirement below:

Note:

This section serves as a cross-referencing matrix only and does not form part of the evaluation/will not be scored independently.

Category	Description	Indicate the section of the proposal that addresses this requirement
Cybersecurity Monitoring and Triage	• Continuous monitoring of all security alerts generated by the in-house (RAF-Owned) Microsoft Sentinel SIEM. • Initial triage to filter false positives and escalate "True Positive" incidents. • Contextualised alerting based on RAF's business risk and asset criticality. • Real-time monitoring and threat detection of the RAF's on-premises and cloud-based systems, applications, and infrastructure. All incidents must be promptly identified, escalated, and addressed. • Monitoring the RAF's environment, including cloud services (AWS, Azure, and Oracle cloud) and on-premises for potential security incidents and unauthorized activity. • Log Management: the SOC should be able to collect and retain logs from multiple systems and generate reports that can be used to provide a holistic view of the environment. • Threat Intelligence Integration: integrate global threat intelligence feeds to detect and respond	

Category	Description	Indicate the section of the proposal that addresses this requirement
	to emerging threats proactively.	
SIEM Engineering & Data Onboarding	The service must provide: • Full management of the SIEM architecture (excluding licensing costs). • Onboarding of new data sources (Syslog, API, Cloud logs, Agents). • Health monitoring of data connectors and log ingestion pipelines to ensure no visibility gaps.	
Detection Engineering & Tuning	The service must provide: • Continuous optimisation and tuning of detection rules to reduce "alert fatigue." • Mapping of all detection use cases to the MITRE ATT&CK Framework. • Custom rule creation based on emerging threats specific to the South African government and insurance sectors. • Leveraging open-source detection use cases such as Sigma.	
Incident Response & SOAR Automation	The service must provide: • Execution of Incident Response (IR) playbooks for containment and eradication. • Implementation and management of SOAR (Security Orchestration, Automation, and Response) to automate repetitive tasks (e.g., blocking IPs, isolating compromised endpoints). • Deep-dive forensic analysis for high-criticality incidents. • Incident Triage and Analysis: prompt triage and analyse security incidents in the environment to	

Category	Description	Indicate the section of the proposal that addresses this requirement
	determine severity, scope, and impact. • Incident Containment and Remediation: contain and remediate security incidents in the environment to minimise their impact and duration, including the execution of Incident Response (IR) playbooks for containment and eradication. • Communication and Coordination: communicate and coordinate with internal and external stakeholders to resolve security incidents and address security risks. • Active Response & Lockdown: In the event of a confirmed breach (like the current stolen access information), the service provider should have the authority to isolate infected machines or lock compromised accounts immediately, through pre-approved TDR actions and operating models. • Root Cause Analysis (RCA): Post-incident investigations to determine how the breach occurred and how to harden the system against future occurrences. • Crisis Management Support: Access to a dedicated Incident Response team for large-scale events.	
Threat Hunting	The service must: • Use advanced security technologies and techniques to conduct ongoing threat hunting activities to identify and mitigate potential security threats in the environment.	

Category	Description	Indicate the section of the proposal that addresses this requirement
	• Provide ongoing threat intelligence and analysis to inform the RAF's security posture and decision-making processes. • Manage Threats: Integrate the RAF's cybersecurity solutions to automate responses to identified threats that pose risks to the RAF environment.	
Threat Response	The service must: • Provide design of implementation of manual, semi-automated and automated responses and recovery actions to detected threats and cyberattacks. • Activate incident response plans in the event of cybersecurity incidents.	
Service Migration	The service must include: • A structured 30-to-60-day transition plan from the current service provider. • Knowledge transfer, migration of existing custom workbooks/dashboards, and validation of current alerting logic.	
Enterprise Integration	The service must: • Cater for threat intelligence integration, to allow for seamless and automated data sharing between the existing security tools and the TDR platform, thus eliminating manual processes and reducing the risk of human error. • Support seamless workflows between existing security tools and the TDR platform thus reducing the time and effort required to switch between different tools and platforms. • Support Single Sign-On (SSO) to reduce the	

Category	Description	Indicate the section of the proposal that addresses this requirement
	time and effort required to log in to multiple tools and platforms. • Support centralised management and monitoring: the integration should allow for centralized management and monitoring of security events, alerts, and incidents, making it easier to track and respond to security incidents. • Allow for the enrichment of data from existing security tools with data from the TDR platform thus providing a more comprehensive and accurate view of security incidents and threats.	
Reporting	The service must: • Provide regular reports to the RAF that provide insight into the performance and effectiveness of its services. The reports must be easy to understand and provide information such as the number of security incidents detected, the number of security incidents resolved, and the time taken to resolve them. • Have a set of metrics in place that measure the performance and effectiveness of its services, including Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). The metrics must align with the SLAs and be used to track and report on the SOC's performance. • Have a performance management process in place that assesses the performance of its services regularly and identifies areas for improvement. The performance management process must be based on the metrics and SLAs and must be used to identify and prioritise areas for improvement.	

Category	Description	Indicate the section of the proposal that addresses this requirement
	• Provide Executive dashboards for Real-time visibility into the organisation's risk score and the status of remediation actions. • Be capable of adapting to the new industry standards. • Include post-incident review and provide detailed reporting on the incident and outcome to relevant stakeholders.	

4.15.2 Professional Services

The successful bidder shall provide implementation, post-implementation professional services, and ongoing support to ensure the secure, stable, and optimised operation of the TDR Solution throughout the contract period.

The service provider must deliver comprehensive technical support to enable RAF to ensure the solution's smooth operation and continuous improvement.

Here are the key aspects of the expected TDR services:

4.15.2.1 Once-off implementation Services

The bidder shall provide comprehensive once-off implementation services, which must include:

- Project initiation and planning, including a detailed implementation plan and project schedule.
- Configuration and optimisation of the solution in alignment with RAF's threat landscape and threat management requirements.
- Integration with RAF ICT systems, including but not limited to:
 - Microsoft Entra ID (Azure AD)
 - RAF Security Logging data sources
 - Identity and Access Management (IAM) and Privileged Access Management (PAM) systems

- Configuration of TDR data sources, data collection rules and data retention policies
- Implementation of TDR use cases and automated response workflows
- Testing, including User Acceptance Testing (UAT).
- Go-live support and hyper-care support for a defined stabilisation period (minimum period to be proposed by bidder).
- The bidder must clearly define:
 - Implementation duration
 - Key deliverables
 - Resource allocation
 - Project governance structure

4.15.2.2 Post Implementation professional services

The bidder is expected to provide 24/7/365 managed TDR services; these professional services may include:

- Advanced configuration changes.
- Threat management detection, response and containment workflow enhancements.
- Integration enhancements.
- Performance tuning to ensure acceptable system responsiveness under normal operational load.
- Cost optimisation
- Technical troubleshooting beyond standard Software as a Service (SaaS) support.
- Threat management and related Advisory workshops.
- Platform optimisation sessions.
- Security configuration adjustments.
- Reporting configuration.

4.15.3 Training and Onboarding

The bidder shall provide comprehensive onboarding and training services to ensure effective adoption and effective use of the Microsoft Sentinel SIEM solution.

4.15.3.1 Technical Training

The bidder must provide technical training for ten (10) cybersecurity personnel. This training must include

- Threat Hunting
- Detection use case development
- Detailed administrator manuals.
- Configuration documentation.
- Escalation procedures.

4.15.3.2 Onboarding and Adoption Support

The bidder must provide onboarding assistance, including:

- Initial system configuration support.
- Data source onboarding.
- Ensuring cost-efficient log ingestion and retention.
- Stabilisation period support.

The bidder must specify:

- Duration of onboarding support.
- Adoption milestones.
- Post-go-live support period.

5 EVALUATION CRITERIA AND METHODOLOGY

The Evaluation Process shall be conducted under the following phases:

Phase 1: Initial Screening Process - All submitted bids will undergo an initial administrative screening to verify compliance with the RAF Request for Bid (RFB) submission requirements, including submission of required returnable documents.

Phase 2: Mandatory Evaluation Process - At this phase Bid Responses are evaluated as per the evaluation criteria specified in the Request for Bid (RFB) document for compliance to Mandatory Requirements. Bidder(s) who met the Mandatory Requirements will be evaluated further on Technical Requirements. Failure to comply with all mandatory requirements will result in disqualification, and such bids will not proceed to Phase 3.

Phase 3: Functionality Evaluation and Service Demonstration

Phase 3 consists of three parts:

- **Part A: Functionality Evaluation** - Bidder(s) must meet the minimum threshold of **70 points out of 100** points allocated at Technical Evaluation to be evaluated further on Part B (Service Demonstration). Only bidders meeting this minimum threshold will proceed to the demonstration/presentation stage.

Part B: Service Demonstration - Shortlisted bidder(s) will be required to deliver a live demonstration of the proposed TDR service in line with section 5.3 of the requirements of this RFB document. Bidders must achieve a minimum score of **50 out of 80** points to proceed to the next stage of the evaluation (Phase 3 Site Visit Phase). Bidders who do not achieve a minimum score of **50 out of 80** points will not be eligible to proceed further with the evaluation and will be disqualified.

Part C: Site Visit - Shortlisted bidders must score **a minimum of 16 out of 20** points for Site visit to be evaluated further on Price and Specific Preference Points Goals).

Phase 4: Price and Specific Goals evaluation - Bidders who successfully meet the required minimum threshold on Phase 3 (Part A, Part B and Part C) will be evaluated on Price; and Specific Goals as per the preferential point system specified in the RFB document.

5.1 MANDATORY REQUIREMENT (PHASE 2)

All Bidders who fail to comply with all Mandatory Requirements will be disqualified and will not proceed to technical evaluation on the functional requirements.

Bidder must indicate compliance by ticking (√) correct box indicating that they either “Comply” OR “Not Comply”

The RAF reserves the right to verify all submitted information.

5.1.1 Mandatory – Operation Center	Comply	Not Comply
The bidder must operate a Security Operations Center within the geographical borders of South Africa. Bidders are required to furnish documentary proof in the name of the bidder indicating physical address such as: • Municipality Statement (Utility bill) not older than 3 months • Valid Lease Agreement/invoices. Where the documentary proof submitted does not clearly match the identity of the bidder, the bidder must submit an explanation on an affidavit for consideration by the RAF.		

Note: Failure to comply with the mandatory requirement shall lead to disqualification.

5.2 TECHNICAL / FUNCTIONAL CRITERIA (PHASE 3 – PART A)

The Technical / Functional Evaluation will be scored out of 100 points.

Bidders must achieve a minimum threshold of **70 out of 100** points to proceed to Phase 3 – Part B (Service Presentation).

Evaluation will be conducted based on the following criteria:

Technical / Functional Criteria	Points
5.2.1 Company Accreditation The bidder must be a Microsoft-accredited partner/reseller, with the following competency: Microsoft Solutions Partner for Security with an Advanced Specialisation in Threat Protection or Cloud Security. Note: The bidder must provide valid (not expired) documentary proof issued by the OEM, confirming the bidder's accreditation or partnership status, in the form of an OEM partnership certificate or letter. The bidder must provide proof of their Microsoft Solutions Partner for Security with an Advanced Specialisation in Threat Protection or Cloud Security. The RAF reserves the right to verify the authenticity of such certification/accreditation with the OEM and/or seek clarity on the partnership status and any other related clarification.	10
5.2.2 Company Track Record The bidder must provide a minimum of three (3) reference letters or 3 references included in a reference table, relating to the Managed SOC, TDR or Managed Detection and Response (MDR) Services within the last seven (7) years. Only reference letters that depict work in the past 7 years from the closing date of the bid will be considered. References may include international implementations of similar scale. Each reference letter must: • Be on the Client's official letterhead. • Indicate the nature of solution and/or services provided. • Indicate the date or year in which the services were rendered (N.B the date on which the letter was signed will not be accepted as the date when the services were rendered). Where the implementation date/year falls on the seventh year from this RFB's closing date, reference letters must include the implementation date with the month/year or day/month/year period, to allow for an accurate evaluation of the period since the services were rendered. • Include contact details for verification.	10

Note: Only reference letters relating to Managed SOC, TDR or Managed Detection and Response (MDR) Services will be considered.

Where reference letters are not available, bidders must provide a list of references relating to the Managed SOC, TDR or Managed Detection and Response (MDR) Services within the last seven (7) years in the following table:

Client	Date/Year	Services Rendered	Client (Name, address and telephone)	Contacts email and

The RAF reserves the right to verify submitted reference letters or the references mentioned in the reference table. Failure to provide complete information for the RAF to verify will result in no scoring of points.

Scoring Matrix	
No. of client's reference letters	Score
No reference letter(s) provided/ No entry on table or submission not relevant	0
One (1) to two (2) reference letters/entry on table provided	5
Three reference letter/entry provided on table provided	10

5.2.3 SOC Personnel and Team Experience (Maximum 15 Points)

15

The bidder must provide CVs of the following personnel:

- Project Manager
- Service Delivery Manager/SOC Manager
- Threat Management Lead (Central Technical Point of Contact)

For each of the above-mentioned personnel, the CVs must clearly highlight areas of competence and years of experience, as well the start date and end date for required experience in the following date format day, month and year or year and month, to enable the relevant experience to be accurately evaluated.

Valid (not expired) copies of relevant qualifications and/or certifications must be provided.

NB! (course/training attendance or completion certificates will not be considered).

Each resource will be evaluated individually, and their combined score will contribute to the total of 15 points.

5.2.3.1 Project Manager

The nominated project manager must meet the following minimum requirements:

- At least five (5) years' ICT Project Management experience,

AND

- Recognised Project Management Certification (e.g. PMBOK, AgilePM, PRINCE 2 or PMP).

OR

Equivalent project management qualification at Diploma level or higher.

NB! Copies of Project Management Certification/qualification(s) must be provided.

Scoring Matrix

Years of experience in ICT Project Management, and Certification/Qualifications of the Project Manager	Score
--	-------

Resource, experience, and certificate(s)/qualifications not provided/ Resource, experience and certificate(s)/qualifications provided do not meet the	0
---	---

minimum requirements		
Resource, experience, and certificate(s)/qualifications provided and meets the minimum requirements.	5	

5.2.3.2 Service Delivery Manager/SOC Manager

The proposed Service Delivery Manager/SOC Manager must meet the following requirements:

- At least five (5) years' experience ICT service delivery management or SOC Management.

AND

- ICT Service Delivery Management Certification/Qualifications such as ITIL v5 higher than ITIL Foundations or COBIT

OR

- Intermediary Cybersecurity Industry certification (CISSP, CRISC or CISM)

NB! Copies of required Certification/qualification(s) must be provided.

Scoring Matrix	
Years of experience in experience ICT service delivery management or SOC Management, and Certification/Qualifications in service delivery management or Cybersecurity	Score
Resource, experience not provided/ Resource, experience provided do not meet the minimum requirements.	0
Resource, experience, and provided and meet the minimum requirements.	5

5.2.3.3 Threat Management Lead

The nominated threat management lead must meet the following minimum requirements:

- At least five (5) years' Threat Management experience

AND

- Cybersecurity Certification (e.g. CISSP, CISM, CRISC, OSCP, CEH or Equivalent).
- SOC/TDR-solution specific certification will be advantageous.

Copies of required Certification/qualification(s) must be provided.

<table border="1"> <tr> <th colspan="2">Scoring Matrix</th></tr> <tr> <th>Years of experience in ICT Project Management, and Certification/Qualifications of the Project Manager</th><th>Score</th></tr> <tr> <td>Resource, experience, and certificate(s)/qualifications not provided/ Resource, experience and certificate(s)/qualifications provided do not meet the minimum requirements</td><td>0</td></tr> <tr> <td>Resource, experience, and certificate(s)/qualifications provided and meets the minimum requirements.</td><td>2.5</td></tr> <tr> <td>Resource, experience, and certificate(s)/qualifications provided and exceeds the minimum requirements (e.g. > 5 years + SOC/TDR-solution-specific certification)</td><td>5</td></tr> </table>		Scoring Matrix		Years of experience in ICT Project Management, and Certification/Qualifications of the Project Manager	Score	Resource, experience, and certificate(s)/qualifications not provided/ Resource, experience and certificate(s)/qualifications provided do not meet the minimum requirements	0	Resource, experience, and certificate(s)/qualifications provided and meets the minimum requirements.	2.5	Resource, experience, and certificate(s)/qualifications provided and exceeds the minimum requirements (e.g. > 5 years + SOC/TDR-solution-specific certification)	5
Scoring Matrix											
Years of experience in ICT Project Management, and Certification/Qualifications of the Project Manager	Score										
Resource, experience, and certificate(s)/qualifications not provided/ Resource, experience and certificate(s)/qualifications provided do not meet the minimum requirements	0										
Resource, experience, and certificate(s)/qualifications provided and meets the minimum requirements.	2.5										
Resource, experience, and certificate(s)/qualifications provided and exceeds the minimum requirements (e.g. > 5 years + SOC/TDR-solution-specific certification)	5										

5.2.4 TDR Service Proposal (Maximum 45 Points)

The bidder must submit a detailed technical proposal addressing the functional requirements.

Scoring will be based on the number of requirements fully met in each category.

The bidder must provide a detailed technical proposal of the Managed TDR services, addressing the functional requirements.

Only requirements clearly addressed in the proposal will be scored.

Category	Description	Scoring Matrix	Points
Cybersecurity Monitoring and Triage	The TDR service must include/address: - Continuous monitoring of all security alerts generated by the in-house (RAF-Owned) Microsoft Sentinel SIEM. - Initial triage to filter false positives and escalate "True Positive" incidents. - Contextualised alerting	0 Points – 1 or No Requirements Met 1 Points – 2 Requirements Met 2 Points – 3 Requirements Met 3 Points – 4 Requirements Met 4 Points – 5 to 6 Requirements Met 5 Points – All 7 Requirements Met	5

	based on RAF's business risk and asset criticality. - Real-time monitoring and threat detection of the RAF's on-premises and cloud-based systems, applications, and infrastructure. - Monitoring the RAF's environment, including cloud services (AWS, Azure, and Oracle cloud) and on premises for potential security incidents and unauthorised activity. - Log Management: the SOC should be able to collect and retain logs from multiple systems and generate reports that can be used to provide a holistic view of the environment. - Threat Intelligence Integration: integrate global threat intelligence feeds to detect and respond to emerging threats proactively.		
SIEM Engineering & Data Onboarding	The TDR service must provide: - Full management of the SIEM architecture (excluding licensing/subscription costs). - Onboarding of new data	0 Points –No Requirement Met 2 Points – 1 Requirement Met 4 Points – 2 Requirements Met 6 Points – All 3 Requirements Met	6

	sources (Syslog, API, Cloud logs, Agents). Health monitoring of data connectors and log ingestion pipelines to ensure no visibility gaps.		
Detection Engineering & Tuning	The TDR service must provide: - Continuous optimisation and tuning of detection rules to reduce "alert fatigue." - Mapping of all detection use cases to the MITRE ATT&CK Framework. - Custom rule creation based on emerging threats specific to the South African government and insurance sectors. - Leveraging open-source detection use cases such as Sigma.	0 Points – No Requirement Met 1 Point – 1 Requirement Met 2 Points – 2 Requirements Met 4 Points – 3 Requirements Met 6 Points – All 4 Requirements Met	6
Incident Response & SOAR Automation	The service must provide: - Execution of Incident Response (IR) playbooks for containment and eradication. - Implementation and management of SOAR (Security Orchestration, Automation, and Response) to automate repetitive tasks (e.g., blocking IPs, isolating compromised endpoints). - Deep-dive forensic analysis for high-criticality incidents.	0 Points – Less than 2 or No Requirement Met 2 Points – 3 Requirements Met 4 Points – 4 to 5 Requirements Met 5 Points – 6 to 7 Requirements Met 6 Points – 8 Requirements Met 7 Points – All 9 Requirements Met	7

	• Incident Triage and Analysis: prompt triage and analyse security incidents in the environment to determine severity, scope, and impact. • Incident Containment and Remediation: contain and remediate security incidents in the environment to minimise their impact and duration, including the execution of Incident Response (IR) playbooks for containment and eradication. • Communication and Coordination: communicate and coordinate with internal and external stakeholders to resolve security incidents and address security risks. • Active Response & Lockdown: In the event of a confirmed breach (like the current stolen access information), the service provider should have the authority to isolate infected machines or lock compromised accounts immediately, through pre-approved TDR actions and operating models. • Root Cause Analysis (RCA): Post-incident investigations to determine how the breach occurred and how to harden the system		
--	---	--	--

	against future occurrences. • Crisis Management Support: Access to a dedicated Incident Response team for large-scale events.		
Threat Hunting	The service must: • Use advanced security technologies and techniques to conduct ongoing threat hunting activities to identify and mitigate potential security threats in the environment. • Provide ongoing threat intelligence and analysis to inform the RAF's security posture and decision-making processes. • Manage Threats: Integrate the RAF's cybersecurity solutions to automate responses to identified threats that pose risks to the RAF environment.	0 Points – No Requirements Met 2 Points – 1 Requirement Met 4 Points – 2 Requirements Met 6 Points – All 3 Requirements Met	6
Threat Response	The service must: • Design and implement manual, semi-automated and automated responses and recovery actions to detected threats and cyberattacks. • Activate incident response plans in the event of cybersecurity incidents.	0 Points – No Requirement Met 3 Points – 1 Requirement Met 6 Points – All 2 Requirements Met	6

Enterprise Integration	The service must: • Cater for threat intelligence integration, to allow for seamless and automated data sharing between the existing security tools and the TDR platform, thus eliminating manual processes and reducing the risk of human error. • Support seamless workflows between existing security tools and the TDR platform thus reducing the time and effort required to switch between different tools and platforms. • Support Single Sign-On (SSO) to reduce the time and effort required to log in to multiple tools and platforms. • Support centralised management and monitoring: the integration should allow for centralized management and monitoring of security events, alerts, and incidents, making it easier to track and respond to security incidents. • Allow for the enrichment of data from existing	0 Points – No Requirements Met 1 Point – 1 Requirement Met 2 Points – 2 Requirements Met 3 Points – All 3 Requirements Met 4 Points – All 4 Requirements Met 5 Points – All 5 Requirements Met	5
------------------------	--	--	---

	security tools with data from the TDR platform thus providing a more comprehensive and accurate view of security incidents and threats.		
Reporting	The service must: • Provide regular reports to the RAF that provide insight into the performance and effectiveness of its services. The reports must be easy to understand and provide information such as the number of security incidents detected, the number of security incidents resolved, and the time taken to resolve them. • Have a set of metrics in place that measure the performance and effectiveness of its services, including Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR). The metrics must align with the SLAs and be used to track and report on the SOC's performance. • Have a performance management process in place that assesses the performance of its services regularly and identifies areas for improvement. The performance management process must be based on the metrics and SLAs and must	0 Points – 1 or No Requirement Met 1 Points – 2 Requirements Met 2 Points – 3 to 4 Requirements Met 3 Points – 5 Requirements Met 4 Points – All 6 Requirements Met	4

	be used to identify and prioritise areas for improvement. • Provide Executive dashboards for Real-time visibility into the organisation's risk score and the status of remediation actions. • Be capable of adapting to the new industry standards. • Include post-incident review and provide detailed reporting on the incident and outcome to relevant stakeholders.		
TOTAL POINTS			45

5.2.4 Managed Services Approach and Transition Plan (Maximum: 15 Points) The bidder must submit, as part of the proposal, a comprehensive project implementation and transition plan, demonstrating how the TDR services will be rolled out, and the TDR platform configured, integrated, and transitioned into operational use at RAF. The plan must clearly address the following: Required Components: i) Detailed project plan with defined phases ii) Clear project activities/milestones and deliverables iii) Defined timelines iv) Identified project resources (roles and responsibilities) v) Implementation methodology (e.g., Agile, PRINCE2, hybrid) vi) Integration approach with RAF Identity & Access Management and ICT environment vii) Data migration/cutover approach (if applicable) viii) Data source onboarding and change management approach ix) Risk management and mitigation strategy during implementation x) Post-implementation stabilisation and support transition plan	15
--	-----------

Scoring Matrix	
Implementation and Transition Plan Quality	Score
No plan provided OR provided plan addresses four (4) or less of the required components.	0
Plan addresses 5 – 6 required components.	5
Plan addresses 7 – 8 required components.	10
Plan addresses 9 – 10 required components.	15

5.2.5 Training and Knowledge Transfer Plan (Maximum: 5 Points) The bidder is required to provide a comprehensive Training and Knowledge Transfer Plan outlining how RAF personnel will be trained and enabled to independently operate and administer the TDR platform. The Plan must clearly address the following: **Required Components:** i) Training plan for Ten (10) RAF personnel ii) Training timelines and duration iii) Delivery method (classroom, virtual, hybrid, self-paced modules) iv) Training materials to be provided (manuals, guides) v) Knowledge transfer plan during the implementation and post-implementation phase vi) Post-implementation knowledge retention strategy	**5**																								
				---	--------------		Scoring Matrix			Training and Knowledge/Skills Transfer Plan	Score		No plan provided OR plan addresses 2 or less of the required components	0		Plan addresses 3 required components	2		Plan addresses 4–5 required components	4		Plan addresses all 6 required components.	5		
TOTAL POINTS																									
Minimum Threshold	**70**																								
Total	**100**																								

Bidders who score a minimum threshold of 70 out of 100 points on Technical/Functional Evaluation (Phase 3 – Part A) will be considered for further evaluation in Phase 3 – Part B (Service Presentation). Bidders who fail to attain the required minimum threshold will not be evaluated further. Only bidders who achieve a minimum score of **50 out of 80 points** during the Service Demonstration (Phase 3 – Part B) will proceed to Phase 3 Part C (Site Visits).

5.3 SERVICE DEMONSTRATION (PHASE 3 PART B)

Shortlisted bidders will be required to provide a live demonstration/presentation of the proposed service to illustrate how the solution meets the solution/technical requirements as outlined in this RFB, specifically those evaluated in the Phase 3 - Part A (Technical Evaluation Section).

Bidders will be given a maximum of five (5) days' notice prior to the demonstrations.

Only functionality demonstrated live will be scored.

NB: Only bidders that meet the minimum threshold of 50 points scored during the service presentation will be evaluated further for Site Visits.

The following will be evaluated during this phase:

Category	Description	Scoring Matrix	Points	Comments
Cybersecurity Monitoring and Triage	The bidder must demonstrate the following capabilities: • Cybersecurity incident triaging workflow/process • Real-time cybersecurity monitoring of TDR data sources • Incident escalation processes and management of false positives	• 0 Points – No Requirement Demonstrated • 2 Points – 1 Requirement Demonstrated • 7 Points – 2 Requirements Demonstrated • 14 Points – All 3 Requirements Demonstrated	14	
Detection Engineering & Tuning	The bidder must demonstrate: • Mapping of detection use cases to the MITRE	• 0 Points – No Requirement Demonstrated	14	

Category	Description	Scoring Matrix	Points	Comments
	ATT&CK Framework. - Custom rule creation based on emerging threats - Leveraging of built-in and customisable open-source detection use cases such as Sigma.	2 Points – 1 Requirement Demonstrated 7 Points – 2 Requirements Demonstrated 14 Points – All 3 Requirements Demonstrated		
Incident Response & SOAR Automation	The service must provide: - Execution of SOAR (Security Orchestration, Automation, and Response) to automate repetitive tasks (e.g., blocking IPs, isolating compromised endpoints). - Deep-dive forensic analysis for high-criticality incidents.	0 Points – No Requirement Demonstrated 2 Points – 1 Requirement Demonstrated 7 Points – 2 Requirements Demonstrated 14 Points – All 3 Requirements Demonstrated	14	

Category	Description	Scoring Matrix	Points	Comments
	Communication and Coordination: communicate and coordinate with internal and external stakeholders to resolve security incidents and address security risks.			
Threat Hunting	The bidder must demonstrate: - Use advanced security technologies and techniques to conduct ongoing threat hunting activities to identify and mitigate potential security threats in the environment. - Provide ongoing threat intelligence and analysis to inform the RAF's security posture and decision-making processes.	0 Points – No Requirement Demonstrated 2 Points – 1 Requirement Demonstrated 7 Points – 2 Requirements Demonstrated 14 Points – All 3 Requirements Demonstrated	14	

Category	Description	Scoring Matrix	Points	Comments
	Manage Threats: Integrate the RAF's cybersecurity solutions to automate responses to identified threats that pose risks to the RAF environment.			
Enterprise Integration	The service must demonstrate: - Integration with a threat intelligence platform/feed, to allow for seamless and automated data sharing between cybersecurity tools and the TDR platform. - Workflows between existing security tools and the TDR platform thus reducing the time and effort required to	0 Points – No Requirement Demonstrated 2 Points – 1 Requirement Demonstrated 7 Points – 2 Requirements Demonstrated 14 Points – All 3 Requirements Demonstrated	14	

Category	Description	Scoring Matrix	Points	Comments
	switch between different tools and platforms. The enrichment of data from existing security tools with data from the TDR platform thus providing a more comprehensive and accurate view of security incidents and threats.			
Reporting	The bidder must demonstrate: - Sample Executive dashboards or reports to provide a centralised view of the threat management posture - Sample metrics to indicate the effectiveness/efficiency of the SOC service, including MTTD and MTTR.	0 Points – No Requirement Demonstrated 5 Points – 1 Requirement Demonstrated 10 Points – All 2 Requirements Demonstrated	10	

Category	Description	Scoring Matrix	Points	Comments
TOTAL POINTS			80	

Service Presentation Total Score Summary

#	Category	Total Maximum Points Scorable	Total Scored at Demonstration	Comments
1	Cybersecurity Monitoring and Triage	14		
2	Detection Engineering & Tuning	14		
3	Incident Response & SOAR Automation	14		
4	Threat Hunting	14		
5	Enterprise Integration	14		
6	Reporting	10		
TOTAL POINTS		80		

Bidders scoring a minimum of 50 points out of 80 points on Live Demonstrations criteria will further be evaluated on site visits.

Phase 3- Part C- Site Visit

The RAF will conduct a physical site visit and inspection of the bidder's Security Operations Centre (SOC). During this evaluation phase, bidders must score a minimum of **16 points out of 20 points** to be evaluated further on Price and Specific Goals. Bidders who do not achieve a minimum of 16 points from the site visit, will be disqualified and not evaluated further on Price and Specific Goals.

Technical Requirements: (Site Visit)	Points	Points scored
Note: Bidders will be evaluated on a site visit on the following:		
SOC Physical access control – The SOC area must be protected through biometric access control.	4	
SOC Physical Segregation – The SOC area must be physically segregated from non-SOC areas through biometric access control.	4	
Power Supply Redundancy – The SOC must be protected against power failure(s) through a backup power supply, which restores power within 5 minutes	4	
Business Continuity Planning - A business continuity plan must be in place to ensure continued business operations and rendering of SOC/TDR services, in the event of a primary SOC site failure.	4	
Fire Protection - The SOC must have a valid certificate of compliance for the fire detection system, and the last service date of the fire detection system is not more than one (1) year from the date of the site visit	4	
SUBTOTAL	20	

5.4 PRICE AND SPECIFIC GOALS (PHASE 4)

The evaluation for Price and Specific Goals shall be based on the 80/20 or 90/10 preference point system and points will be allocated as follows:

Evaluation criteria					Points
1.	Price				80/90
2.	Specific Goals				20/10
	#	Specific Goal	Proof	Points Allocation	
	1	South African citizen who had no franchise in national elections prior to the introduction of the Constitution of the Republic of South Africa, 1983 (Act 200 of 1983) or the Constitution of the Republic of South Africa, 1996. (Minimum 51% ownership or more)	CSD Report	10/5	
	2	Women Ownership (minimum 51% ownership or more)	ID copy / CSD report	8/4	
	3	Persons with disabilities (minimum 51% ownership or more)	Valid medical certificate issued by an accredited medical practitioner.	2/1	

5.5 PRICING SCHEDULE

This annexure should be completed and signed by the Bidder's authorised personnel.

NB: PLEASE PROVIDE COST BREAK-DOWN FOR EACH DELIVERABLE IN SEPARATE PAGE WITH NO TERMS AND CONDITIONS.

All prices must be VAT inclusive and must be quoted in South African Rand (ZAR). The pricing will be added to determine the total cost of the services for comparison purposes to award the bid.

Total Contract Value

The Total 5-Year Contract Value shall consist only of:

- 24/7/365 Managed TDR services for five (5) years
- TDR data source onboarding
- TDR configuration and tuning
- Once-off implementation costs.
- Training and skills/knowledge transfer costs.
- TDR platform support costs

Please indicate your total bid price here (five-year contract value - (VAT inclusive) R..... (Compulsory)

Important: It is mandatory to indicate your total bid price as requested above. This price must be the same as the total bid price you submit in your pricing schedule. Should the total bid prices differ, the one indicated above shall prevail for evaluation purposes.

5.6 Escalation and Pricing Principles

- 1) Subscription pricing for Years 2–5 must either:
 - a) Remain fixed for the entire five (5) year contract period, OR
 - b) Be subject to a fixed annual escalation percentage declared at bid stage.
- 2) Where escalation is applied:
 - The escalation percentage must be fixed and capped.
 - CPI-linked, floating, market-adjusted, foreign exchange adjusted, or index-linked escalation formulas will not be accepted.
 - Escalation must apply uniformly across all recurring subscription components.

- 3) If no escalation percentage is disclosed, pricing will be deemed fixed for the full five (5) year period.
- 4) All pricing must include any costs associated with:
 - Project management
 - SOC personnel
 - Security controls
 - Integration
 - Compliance requirements
 - Reporting capabilities
- 5) No additional platform fees, administrative fees, pass-through costs, third-party charges, currency adjustments, or hidden costs will be accepted outside this pricing schedule unless formally approved through contract variation procedures in accordance with applicable procurement legislation and in line with RAF policies, at the sole discretion of RAF.

5.7 Managed TDR Services Pricing

Deliverables	Price Year 1 Base Price (TDR Implementation, Configuration and Optimisation)	Escalation % (if applicable)	Price Year 2	Price Year 3	Price Year 4	Price Year 5	Total Five-Year Value
Managed TDR Services	R	__% OR Fixed	R	R	R	R	R

5.8 Once-Off Costs (No Escalation Permitted)

These costs must be fixed and applicable only in Year 1.

Item	Year 1 Price	Notes
Implementation & Configuration	R	Fixed
Formal Training (10 Personnel)	R	Fixed
Data Migration (If applicable)	R	Fixed

Data Source Onboarding	R	
Total Once-Off Costs	R	

Important:

- In the event of any discrepancy between the annual breakdown and the stated Total 5-Year Contract Value, the Total 5-Year Contract Value shall prevail for evaluation purposes.
- Bidders are responsible for ensuring arithmetic accuracy. RAF reserves the right to correct obvious arithmetical errors in accordance with applicable procurement regulations.

Bidder's Name:

Signature:

Date:

NATIONAL TREASURY

Republic of South Africa



GOVERNMENT PROCUREMENT: GENERAL CONDITIONS OF CONTRACT

July 2010

NOTES

The purpose of this document is to:

- (i) Draw special attention to certain general conditions applicable to government bids, contracts and orders; and
- (ii) To ensure that clients be familiar with regard to the rights and obligations of all parties involved in doing business with government.

In this document words in the singular also mean in the plural and vice versa and words in the masculine also mean in the feminine and neuter.

- The General Conditions of Contract will form part of all bid documents and may not be amended.
- Special Conditions of Contract (SCC) relevant to a specific bid, should be compiled separately for every bid (if applicable) and will supplement the General Conditions of Contract. Whenever there is a conflict, the provisions in the SCC shall prevail.

TABLE OF CLAUSES

1. Definitions
2. Application
3. General
4. Standards
5. Use of contract documents and information; inspection
6. Patent rights
7. Performance security
8. Inspections, tests and analysis
9. Packing
10. Delivery and documents
11. Insurance
12. Transportation
13. Incidental services
14. Spare parts
15. Warranty
16. Payment
17. Prices
18. Contract amendments
19. Assignment
20. Subcontracts
21. Delays in the supplier's performance
22. Penalties
23. Termination for default
24. Dumping and countervailing duties
25. Force Majeure
26. Termination for insolvency
27. Settlement of disputes
28. Limitation of liability
29. Governing language
30. Applicable law
31. Notices
32. Taxes and duties
33. National Industrial Participation Programme (NIPP)
34. Prohibition of restrictive practices

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 Department or an organization acting on behalf of the Department.
- 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 | <p>16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in SCC.</p> <p>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.</p> <p>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.</p> <p>16.4 Payment will be made in Rand unless otherwise stipulated in SCC.</p> |
| 17. Prices | <p>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.</p> |
| 18. Contract amendments | <p>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.</p> |
| 19. Assignment | <p>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.</p> |
| 20. Subcontracts | <p>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.</p> |
| 21. Delays in the supplier's performance | <p>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.</p> <p>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.</p> <p>21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national department, provincial department, or a local authority.</p> <p>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</p> |

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 canceling 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 anti-dumping 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 Department 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 Department 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.

- 34.3 If a bidder(s) or contractor(s), has / have been found guilty by the Competition Commission of the restrictive practice referred to above, the purchaser may, in addition and without prejudice to any other remedy provided for, invalidate the bid(s) for such item(s) offered, and / or terminate the contract in whole or part, and / or restrict the bidder(s) or contractor(s) from conducting business with the public sector for a period not exceeding ten (10) years and / or claim damages from the bidder(s) or contractor(s) concerned.