

APPOINTMENT OF A SUITABLE SERVICE PROVIDER TO DELIVER A COMPREHENSIVE INFORMATION AND COMMUNICATION TECHNOLOGY(ICT) MANAGED SECURITY SERVICES FOR A PERIOD OF 36 MONTHS WITHIN THE OFFICE OF THE VALUER-GENERAL.

THERE WILL BE A **COMPULSORY BRIEFING SESSION** AS FOLLOWS:

DATE: **TUESDAY, 03 MARCH 2026**

TIME: 11:00

LOCATION: Praetor Forum Building

3rd Floor, 267 Lilian Ngoyi Street

Pretoria, 0001

[GPS Coordinates](#)

**BID RESPONSE DOCUMENTS MUST BE DEPOSITED IN THE BID BOX SITUATED AT:
OFFICE OF THE VALUER-GENERAL (OVG)**

Praetor Forum Building

3rd Floor, 267 Lilian Ngoyi Street

Pretoria, 0001

[GPS Coordinates](#)

CLOSING DATE: MONDAY, 16 MARCH 2026 AT 11:00

ENQUIRIES PLEASE CONTACT: TECHNICAL RELATED:

No.	Office	Contact person	Contact details
1.	Office of the Valuer-General	Mrs J Modisamongwe	060 535 5778 Johanna.Modisamongwe@ovg.org.za
2.	Office of the Valuer-General	Ms M Maisa	069 019 5019 Mathabo.Maisa@ovg.org.za

BID RELATED:

No.	Contact Person	Contact Details
1	Mr. GI Sekwale: +27 12 036 3036	ovgscp@ovg.org.za
2.	Ms. K Seatlholo: +27 12 036 3024	



YOU ARE HEREBY INVITED TO BID TO THE OFFICE OF THE VALUER GENERAL

BID NO: OVG (02) 2025/2026 **CLOSING TIME:** 11:00 **CLOSING DATE:** MONDAY, 16 MARCH 2026

BIDS RECEIVED AFTER THE CLOSING TIME AND DATE AS A RULE WILL NOT BE ACCEPTED FOR CONSIDERATION

1. Kindly furnish us with a bid for services shown on the attached forms.

2. Attached please find:

2.1 Authority to Sign the Standard Bidding Documents (SBDs) on behalf of an Entity	 Page 3 – 4
2.2 Invitation to Bid – SBD 1	 Page 5 – 6
2.3 Pricing Schedule (Services) – SBD 3.3	 Page 7 - 9
2.4 Declaration of Interest – SBD 4	 Page 10 - 12
2.5 Preference Points Claim Form – SBD 6.1	 Page 12 - 16
2.8 OVG Supplier Maintenance (Bank Details) Form	 Page 17 - 19
2.9 Terms of Reference	 Page 20 - 44
2.10 General Conditions of Contract (GCC)	 Page 45 – 58

3. If you are a sole agent or sole supplier you should indicate your market price after discount to your other clients or if that is not possible your percentage net profit before tax, to decide whether the price quoted is fair and reasonable.

3.1.1 The attached forms must be completed in detail and returned with your bid. Failure to comply may disqualify your proposal. Bid document must be submitted in a sealed envelope stipulating the following information: Name and Address of the bidder, Bid number and closing date of bid.

**Bid proposals must be deposited into the Tender/ Bid Box situated at the Reception Area at the physical address: OFFICE OF THE VALUER-GENERAL
267 Praetor Building, 3rd Floor, Cnr Pretorius and Lilian Ngoyi Street, Pretoria, 0001**

by not later than the closing date and time indicated above. Bid proposals which are not inside the Tender/ Bid Box on the closing date and time will not be considered

By participating in this bid, you are accepting to have your Personal Information published on the websites (OVG/National Treasury) for purposes of enhancing compliance, monitoring, and improving transparency and accountability within Supply Chain Management.

Yours faithfully

SUPPLY CHAIN MANAGEMENT (SCM)



+27 12 036 0000/2



Private Bag X 874,
Pretoria, 0001



267 Praetor Forum Building, 3rd Floor,
Cnr Pretorius & Lillian Ngoyi Street,
Pretoria, 0001



vg@ovg.org.za



www.ovg.org.za

AUTHORITY TO SIGN THE STANDARD BIDDING DOCUMENTS (SBD) ON BEHALF OF AN ENTITY.

“Only authorized signatories may sign the original and all copies of the tender offer where required.

In the case of a **ONE-PERSON CONCERN** submitting a tender, this shall be clearly stated.

In case of a **COMPANY** submitting a tender, include a copy of a **resolution by its board of directors** authorizing a director or other official of the company to sign the documents on behalf of the company.

In the case of a **CLOSED CORPORATION** submitting a tender, include a copy of a **resolution by its members** authorizing a member or other official of the corporation to sign the documents on each member's behalf.

In the case of a **PARTNERSHIP** submitting a tender, **all the partners shall** sign the documents, unless one partner or a group of partners has been authorized to sign on behalf of each partner, in which case **proof of such authorization** shall be included in the Tender.

In the case of a **JOINT VENTURE** submitting a tender, include **a resolution** of each company of the Joint Venture together with a resolution by its members authorizing a member of the Joint Venture to sign the documents on behalf of the Joint Venture.”

Accept that failure to submit proof of Authorization to sign the tender shall result in a Tender Offer being regarded as non-responsive.

AUTHORITY OF SIGNATORY

Signatories for companies, closed corporations and partnerships must establish their authority **BY ATTACHING TO THIS FORM, ON THEIR ORGANISATIONS'S LETTERHEAD STATIONERY**, a copy of the relevant resolution by their Board of Directors, Members or Partners, duly signed and dated.

An **EXAMPLE** is shown below for a COMPANY:

MABEL HOUSE (Pty) Ltd	
By resolution of the Board of Directors taken on <i>20 May 2000</i> ,	
MR A.F JONES	
has been duly authorised to sign all documents in connection with	
Contract no CRDP 0006, and any contract which may arise there from,	
on behalf of <i>Mabel House (Pty) Ltd.</i>	
SIGNED ON BEHALF OF THE COMPANY:	(Signature of Managing Director)
IN HIS CAPACITY AS:	Managing Director
DATE:	20 May 2000
SIGNATURE OF SIGNATORY:	(Signature of A.F Jones)
As witnesses:	
1.	
2.	
Signature of person authorised to sign the tender:	
Date:	

PART A INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE OFFICE OF THE VALUER GENERAL (OVG)					
BID NUMBER:	OVG (02) 2025/2026	CLOSING DATE:	16 MARCH 2026	CLOSING TIME:	11:00 AM
DESCRIPTION	APPOINTMENT OF A SUITABLE SERVICE PROVIDER TO DELIVER A COMPREHENSIVE INFORMATION AND COMMUNICATION TECHNOLOGY(ICT) MANAGED SECURITY SERVICES FOR A PERIOD OF 36 MONTHS WITHIN THE OFFICE OF THE VALUER-GENERAL.				
BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT: GPS Coordinates					
OFFICE OF THE VALUER-GENERAL (OVG)					
267 Praetor Building, 3 rd Floor, Cnr Pretorius and Lilian Ngoyi Street					
PRETORIA					
0001					
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO			TECHNICAL ENQUIRIES MAY BE DIRECTED TO:		
CONTACT PERSON	Mr GISekwale/ Ms K Seatlholo		CONTACT PERSON	Mrs. J Modisamongwe/ Ms M Maisa	
TELEPHONE NUMBER	012 036 3036/ 3024		TELEPHONE NUMBER	060 535 5778	
FACSIMILE NUMBER	N/A		FACSIMILE NUMBER	N/A	
E-MAIL ADDRESS	ovgscp@ovg.org.za		E-MAIL ADDRESS	Mathabo.Maisa@ovg.org.za Johannah.Modisamongwe@ovg.org.za	
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
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE	TICK APPLICABLE BOX] ☐ Yes ☐ No		B-BBEE STATUS LEVEL SWORN AFFIDAVIT		[TICK APPLICABLE BOX] ☐ Yes ☐ No
[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/ SWORN AFFIDAVIT (FOR EMES & QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]					
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	☐ Yes ☐ No [IF YES ENCLOSE PROOF]		ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES /WORKS OFFERED?		☐ Yes ☐ No [IF YES, ANSWER 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).
1.5. By participating in this bid, you are accepting to have your Personal Information published on the websites (OVG/National Treasury) for purposes of enhancing compliance, monitoring, and improving transparency and accountability within Supply Chain Management.
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)

DATE:

PRICING SCHEDULE [SBD 3.3]

PRICING SCHEDULE [SBD 3.3]

(Services)

NAME OF BIDDER:

BID NO.: OVG (02) 2025/2026

CLOSING DATE: 16 MARCH 2026

CLOSING TIME: 11H00 AM

OFFER TO BE VALID FOR **90 DAYS** FROM THE CLOSING DATE OF BID.

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

NB: PRICING SHOULD REMAIN FIXED AND INCLUSIVE OF VAT IF REGISTERED AS VAT VENDORS.

Item No	Description	Quantity	Cost Per Unit	Total Cost (Excluding 15% Vat)
1.	Installation, Configuration and Deployment (As per Table 2: Scope of Work)	Once-off	R	R
	1. TOTAL COST FOR INSTALLATION, CONFIGURATION AND DEPLOYMENT SERVICES			R
2.	Cloud Hosting Service: (As per Table 2: Scope of Work)			
	Year 1	12 months	R	R
	Year 2	12 months	R	R
	Year 3	12 months	R	R
	2. TOTAL CLOUD HOSTING SERVICE COST FOR 36 MONTHS			R
3.	SECURITY SOFTWARE AND TOOLS (As per Table 2: Scope of Work)			
	3.1 Software Licenses			
	Year 1	12 months	R	R
	Year 2	12 months	R	R
	Year 3	12 months	R	R
	3.1 Total Software License for 36 Months			R
	3.2 Onsite Hardware License			
	Year 1	12 months	R	R
	Year 2	12 months	R	R
	Year 3	12 months	R	R

Initials

Date:

PRICING SCHEDULE [SBD 3.3]

	3.2 Total Onsite Hardware License for 36 Months			R
	3. TOTAL SECURITY SOFTWARE AND TOOLS COST for 36 Months (3.1 & 3.2)			R
Item No	Description	Quantity	Cost Per Unit	Total Cost (Excluding 15% Vat)
4.	ADVANCED ELECTRONIC SIGNATURES SOFTWARE LICENSE (50 X CONCURRENT LICENCES) (AS PER TABLE 2: SCOPE OF WORK)			
	Year1	12 months	R	R
	Year 2	12 months	R	R
	Year 3	12 months	R	R
	4. TOTAL ADVANCED ELECTRONIC SIGNATURES SOFTWARE LICENSE COST FOR 36 MONTHS			R
5.	CYBERSECURITY SUPPORT AND MONITORING (AS PER TABLE 2: SCOPE OF WORK)			
	Year1	12 months	R	R
	Year 2	12 months	R	R
	Year 3	12 months	R	R
	5. TOTAL CYBERSECURITY SUPPORT AND MONITORING COST FOR 36 MONTHS			R
6.	DISASTER RECOVERY AND BACKUPS (AS PER TABLE 2: SCOPE OF WORK)			
	6.1 Disaster Recovery Service			
	Year1	12 months	R	R
	Year 2	12 months	R	R
	Year 3	12 months	R	R
	6.1 TOTAL DISASTER RECOVERY SERVICE FOR 36 MONTHS			R
	6.2 Backup/Storage Service			
	Year1	12 months	R	R
	Year 2	12 months	R	R
	Year 3	12 Months	R	R
	6.2 TOTAL BACKUP/STORAGE SERVICE FOR 36 MONTHS			R
	6. TOTAL DISASTER RECOVERY AND BACKUPS SERVICES COST (6.1 & 6.2)			R
7.	TRAINING			
	7.1 Training (As per Table 2: Scope of Work)	Once Off		

Initials

Date:

PRICING SCHEDULE [SBD 3.3]

		6 x ICT personnel	R	R
	7.1 TOTAL COST FOR TRAINING 6 X ICT PERSONNEL			R
	Description	Quantity	Cost Per Unit	Total Cost (Excluding 15% Vat)
	7.2 Cybersecurity Awareness and Training (Bi-annually for three years)			
	Cybersecurity Awareness	Bi-annual for 3 Years	R	R
	7.2 TOTAL COST FOR CYBERSECURITY AWARENESS(BI-ANNUALLY)			R
	7. TOTAL COST FOR TRAINING (7.1 & 7.2)		R	
SUB –TOTAL (1- 7) Excluding 15% VAT)			R	
15% VAT			R	
Total (15% VAT Incl.)			R	

NB: FAILURE TO FULLY COMPLETE THIS SBD 3.3 WILL RENDER YOUR PROPOSAL REGARDED AS NON-RESPONSIVE AND WILL THEREFORE NOT BE CONSIDERED FOR FURTHER EVALUATION.

NB! The OVG will process invoice payments upon the successful completion of the abovementioned deliverables in line with the approved project plan.

NB! The OVG will not accept changes to the pricing post implementation that arise due to the service provider underquoting or overlooking any costing elements. Where projections are made for example annual price escalations, and the actual rate becomes more than the projected cost, the amount indicated in this schedule will be used for invoicing, and no amendments will be accepted.

Initials

Date:

BIDDER'S DISCLOSURE

1. PURPOSE OF THE FORM

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

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

2. Bidder's declaration

- 2.1 Is the bidder, or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest¹ in the enterprise, employed by the state? **YES/NO**

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

Full Name	Identity Number	Name of State institution

- 2.2 Do you, or any person connected with the bidder, have a relationship

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

with any person who is employed by the procuring institution? **YES/NO**

2.2.1 If so, furnish particulars:

.....

2.3 Does the bidder or any of its directors / trustees / shareholders / members / partners or any person having a controlling interest in the enterprise have any interest in any other related enterprise whether or not they are bidding for this contract? **YES/NO**

2.3.1 If so, furnish particulars:

.....

3 DECLARATION

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

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

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

institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.

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

I CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 1, 2 and 3 ABOVE IS CORRECT.

I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME IN TERMS OF PARAGRAPH 6 OF PFMA SCM INSTRUCTION 03 OF 2021/22 ON PREVENTING AND COMBATING ABUSE IN THE SUPPLY CHAIN MANAGEMENT SYSTEM SHOULD THIS DECLARATION PROVE TO BE FALSE.

.....	
Signature	Date
.....	
Position	Name of bidder

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

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

- (a) Price; and
- (b) Specific Goals.

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

The maximum points for this tender are allocated as follows:

	POINTS
PRICE	
SPECIFIC GOALS	
Total points for Price and SPECIFIC GOALS	100

- 1.5 Failure on the part of a tenderer to submit proof or documentation required in terms of this tender to claim points for specific goals with the tender, will be interpreted to mean that preference points for specific goals are not claimed.
- 1.6 The organ of state reserves the right to require of a tenderer, either before a tender is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the organ of state.

2. DEFINITIONS

- (a) “**tender**” means a written offer in the form determined by an organ of state in response to an invitation to provide goods or services through price quotations, competitive tendering process or any other method envisaged in legislation;
- (b) “**price**” means an amount of money tendered for goods or services, and includes all applicable taxes less all unconditional discounts;
- (c) “**rand value**” means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;
- (d) “**tender for income-generating contracts**” means a written offer in the form determined by an organ of state in response to an invitation for the origination of income-generating contracts through any method envisaged in legislation that will result in a legal agreement between the organ of state and a third party that produces revenue for the organ of state, and includes, but is not limited to, leasing and disposal of assets and concession contracts, excluding direct sales and disposal of assets through public auctions; and
- (e) “**the Act**” means the Preferential Procurement Policy Framework Act, 2000 (Act No. 5 of 2000).

3. FORMULAE FOR PROCUREMENT OF GOODS AND SERVICES

3.1. POINTS AWARDED FOR PRICE

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

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

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

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:

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

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 claimed (80/20 system) (To be completed by the tenderer)
HDIs who had no franchise in the elections before 1983 and 1993 Constitution	10	
HDIs who is a Female	5	
People with Disabilities (PwDs)	5	
Total	20	

NB: Bidders are required to submit proof of HDI. Proof includes valid Central Supplier Database (CSD) together with their tenders to substantiate their specific Goals claims for HDIs.

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:	
	
	
	



SUPPLIER MAINTENANCE

☐

SAGE

System User Only	
Captured By:	
Captured Date:	
Authorized By:	
Date Authorized:	
Safety Web Verification	
YES	NO

Office

The office of the Valuer-General

☐☐

I/We hereby request and authorize you to pay any amounts which may accrue to me/us to the credit of my/our account with the mentioned bank. I/we understand that the credit transfers hereby authorized will be processed by computer through a system known as "ACB - Electronic Fund Transfer Service", and I/we understand that not additional advice of payment will be provided by my/our bank, but that the details of each payment will be printed on my/our bank statement or any accompanying voucher. (This does not apply where it is not customary for banks to furnish bank statements).

I/we understand that the OVG will supply payment advice in the normal way, and that it will indicate the date on which the funds will be made available on my/our account.

This authority may be cancelled by me/us by giving thirty days' notice by prepaid registered post. Please ensure information is valid as per required bank screens.

I/We understand that bank details provided should be exactly as per the records held by the bank.

I/We understand that the OVG will not assume responsibility for any delayed payments, as a result of incorrect information supplied.

Company / Personal Details

Registered Name	
Trading Name	
Tax number	
Vat Number	
CSD Supplier Number	
Title	
Initials	
First Names (as per id)	
Surname	

Address Detail

Postal Address Line 1	
Postal Address Line 2	
Physical Address Line 1	
Physical Address Line 2	
Postal Code	



+27 12 036 0000/2



Private Bag X 874,
Pretoria, 0001



267 Praetor Forum Building, 3rd Floor,
Cnr Pretorius & Lillian Ngoyi Street,
Pretoria, 0001



vg@ovg.org.za



www.ovg.org.za

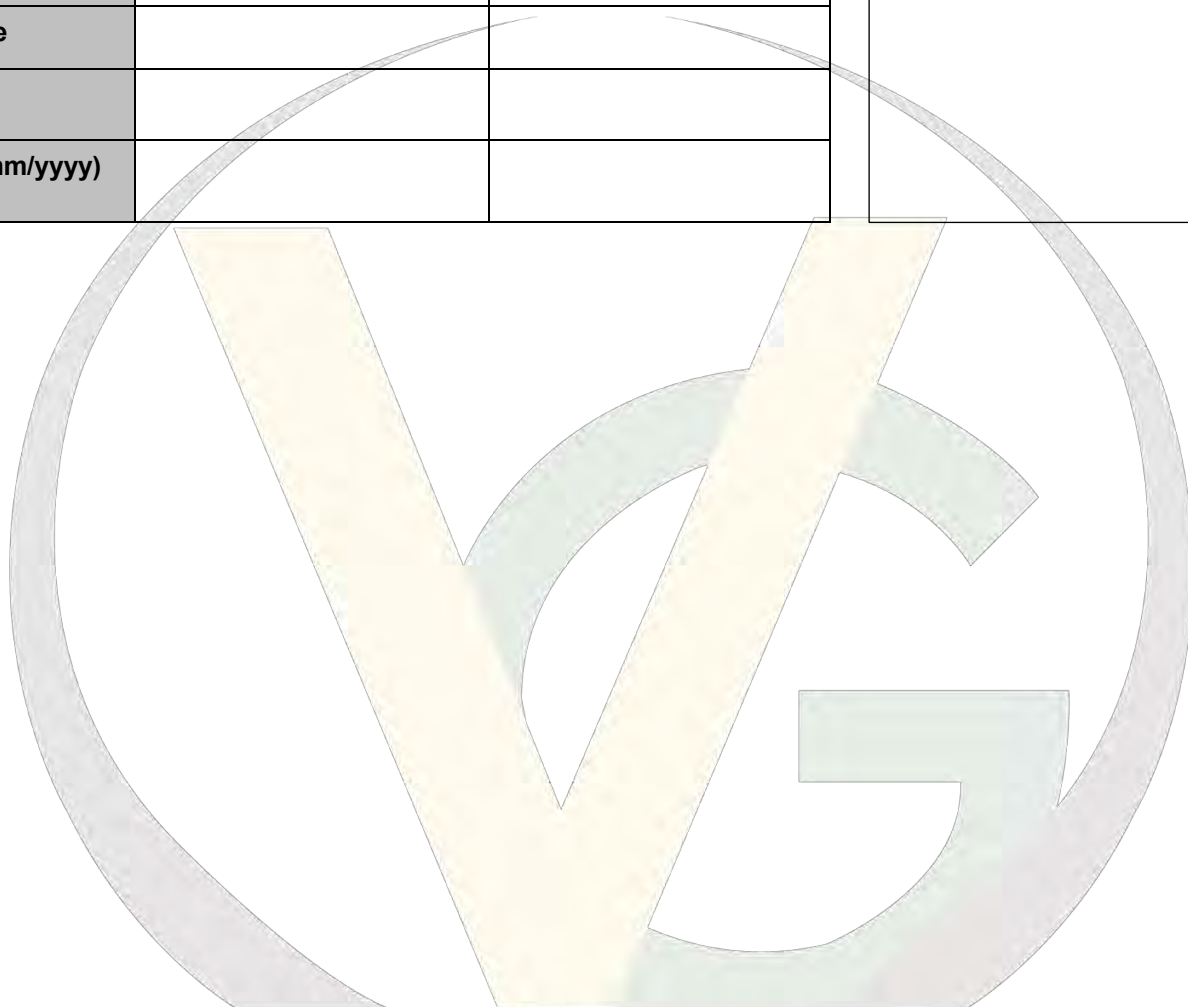
New Supplier Information ☐		Update Supplier Information ☐	
Supplier Type	Individual ☐	Department ☐	Department Number
	Company ☐	Trust ☐	Other Specify:
	CC ☐	Other ☐	
	Partnership ☐		

Supplier Bank Account Details	
This field is compulsory and should be accompanied by not older than 3 months bank account confirmation letter	
Account Holder	
Account Number	
Branch Name	
Branch Number	
Account Type	☐ Cheque/Current Account ☐ Savings Account Transmission ☐ Account Bond Account ☐ Other (Please Specify)
ID Number	
Passport Number	
Company Registration Number	
*CC Registration	
* Please include CC/CK where applicable	
Practice Number	
Not older than 3 months bank account confirmation letter It is hereby confirmed that this detail has been verified against the following screens ABSA -CIF screen FNB -Hogan's system on the CIS4 STD Bank-Look-up-screen Nedbank - Banking Platform under the Client Details Tab	
CSD Bank Verification Status (Banking details must appear on Central Supplier Database)	Verification Succeeded Yes ☐ No ☐

Contact Details			
Business			
Home Fax	Area Code	Telephone Number	Extension
Cell	Area Code	Telephone Number	Extension
	Area Code	Telephone Number	
	Cell Code	Cell Number	
E-mail Address			
Contact Person			

	Supplier details	Organization sender details
Signature		
Print Name		
Rank		
Date (dd/mm/yyyy)		

Address of the Office of the Valuer General
where form is submitted from:





TERMS OF REFERENCE FOR THE APPOINTMENT OF A SUITABLE SERVICE PROVIDER TO DELIVER A COMPREHENSIVE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) MANAGED SECURITY SERVICES FOR A PERIOD OF 36 MONTHS WITHIN THE OFFICE OF THE VALUER-GENERAL.

1. PURPOSE

- 1.1 The Office of the Valuer-General (OVG) seeks to appoint an experienced bidder for managed security services. The services include providing end-to-end remote Managed Security Services from Detection to Remediation, cybersecurity posture, optimised disaster recovery capabilities, robust data protection solution and support.

2. INTRODUCTION AND BACKGROUND

- 2.1 The OVG is a Schedule 3A state entity established in terms of the Property Valuation Act No.17 of 2014 (PVA) and its listing as a National Public Entity is in terms of the Public Finance Management Act.
- 2.2 The organisation has the mandate of supporting the programme of Land Reform through providing independent and credible property valuation services. It is envisaged that, through the mandate specifically designed for this entity, land claim valuations will be settled with greater efficiency and decisiveness, thereby speeding up the process of Land Reform.
- 2.3 The OVG currently has a workforce of 92 employees and projects headcount growth to approximately 150 employees over the next three to five years.
- 2.4 The below section outlines the current OVG ICT environment:
- 2.4.1 The organisation seeks to implement a managed security solution to ensure it is effectively protecting its assets availability, confidentiality, and integrity against vulnerabilities and threats. However, recognizing the evolving landscape of cybersecurity threats and the need for a more comprehensive and independent ICT infrastructure, the OVG has taken a proactive step towards enhancing its capabilities.



+27 12 036 0000/2



Private Bag X 874,
Pretoria, 0001



267 Praetor Forum Building, 3rd Floor,
Cnr Pretorius & Lilian Ngoyi Street,
Pretoria, 0001



vg@ovg.org.za



www.ovg.org.za

2.4.2 As part of this strategic initiative, the organisation has successfully completed the upgrade of its server room, ensuring a data centre environment for hosting critical IT assets and implemented the Enterprise Resource Planning, (ERP) system which supports the Financial Management, Asset Management, Human Resources Management, Supply Chain Management, Valuation Management Business processes, Active Directory and Monitoring systems.

2.4.3 Furthermore, the organisation has invested in additional servers, which are hosted on-premises, signifying a move towards greater autonomy and control over its ICT infrastructure and applications.

2.4.4 To build on this foundation and to address the growing importance of cybersecurity, currently embarking on a comprehensive project. This project encompasses three key service definitions, each designed to enhance the OVG's cybersecurity posture, optimised disaster recovery capabilities, and implement a robust data protection system.

Table 1: Current ICT Environment

Current ICT Environment	
Devices	
Laptops	150
Servers	10 Physical hosts and 14 Virtual Machines (growth included)
Printers	2
Network Switches	7
ERP application servers	6
ERP database	1
Monitoring and Deployment Server	2
Mobile phones	92
Cloud Services	2
Number of Users	92

3. SCOPE OF WORK

3.1 Table 2: illustrates the scope of activities as follows.

Table 2: Scope of Work

Focal points	Requirements
--------------	--------------

The proposed solution must incorporate the following information security domains:

1. Identity and access management
2. Data protection and privacy
3. End point security
4. Application security
5. Cyber security
6. Disaster recovery
7. Cloud Security

1. Identity and Access Management	1.1 The solution must provide audit logging of all access activities and authentication activities, including successful and failed login attempts, privilege escalations, and administrative actions. 1.2 Must support cryptographic protocols such as Multifactor Factor Authentication (MFA) and Single Sign On (SSO) within authentication and authorisation. 1.3 Ensure secure protocols such as SAML, OAuth are implemented to protect credentials through encryption and signature. 1.4 Provide enhanced controls for managing administrative and high-risk accounts. 1.5 Must include real-time monitoring and correlation of access events for anomaly detection and potential security incidents. 1.6 Must provide automated provisioning and deprovisioning. 1.7 Must integrate with cloud services and third-party applications such as Enterprise Resource Planning (ERP). 1.8 Must support Role-Based Access Control (RBAC) to ensure users have the minimum necessary privileges (principle of least privilege). 1.9 Ability to provide notifications e.g. email based. 1.10 Must retain audit logs in compliance with organisational policies and applicable data protection regulations. 1.11 The solution must allow integration with Security Information and Event Management (SIEM) platform for centralised monitoring.
2. Endpoint Security	Provide Endpoint Security Solution to all OVG Endpoints including servers. 2.1 The bidder must implement extended detection and response (XDR) solution for real-time threats analysis. 2.2 The solution must support operating systems

	Windows 10, 11, Windows Server 2016, 2019 to WinServer 2025. 2.3 The proposed solution must support the below virtual platforms: VMware ESXi 8.0 Update 2, MS Hyper-V Server 2019 to 2025. 2.4 The proposed solution must be able to detect security threats (e.g Viruses, Worms, Trojans). 2.5 The proposed solution must be able to integrate with Windows Defender Security Centre. 2.6 The proposed solution must provide Memory Scanning for Windows workstations. 2.7 The proposed solution should be able to protect or manage mobile devices including Android and iOS. 2.8 Implement encryption for data in transit. 2.9 Integrate endpoint logs with SIEM for threat analysis. 2.10 Generate endpoint security reports on threats, vulnerabilities, and patch status.
3. Application Security	3.1 Deploy Web Application Firewall (WAF) to protect against external threats. 3.2 Encrypt sensitive data at rest and in transit using SSL/TLS and AES encryption. 3.3 Integrate application logs with SIEM tool. 3.4 Monitor applications for anomalous activities and unauthorised access.
4. Email Security	The bidder must provide and implement the Email security solutions that includes: 4.1 The solution must provide multi-layered protection against email threats such as phishing, spoofing, malware and zero-day attacks. 4.2 The solution must use Artificial Intelligence/Machine Learning (AI/ML), sandboxing and global threat intelligence to detect and block malicious attachments, links, and hidden code/payloads. 4.3 The solution must verify the authenticity of email senders using standards like SPF, DKIM, and DMARC to prevent impersonation or fraudulent emails. 4.4 The solution must provide email encryption to ensure sensitive and confidential information is protected both whiles being sent in transit and when stored at rest. 4.5 The solution must support Data Loss Prevention (DLP) policies to prevent accidental or unauthorized sharing of sensitive information

	(e.g., financial data, personal information, or classified records). 4.6 The solution must check links at the time a user clicks them ("time-of-click analysis") to stop access to malicious websites. 4.7 The solution must integrate seamlessly with Microsoft 365 (Exchange Online/Outlook) to provide continuous protection without disrupting user experience. 4.8 The solution must provide impersonation detection capabilities to safeguard executives and high-value targets from social engineering attacks. 4.9 The solution must allow integration with Security Information and Event Management (SIEM) platform for centralised monitoring.
5. Cyber security monitoring	The following managed security service features must be present in the bidder's solution: 5.1 The solution must provide real-time monitoring of cybersecurity events on a 24/7/365 basis to ensure constant visibility into threats and risks. 5.2 The solution must monitor and analyse system, application, and network activity logs to detect suspicious or unauthorised activities that may indicate a potential security incident. 5.3 The solution must include capabilities to detect, investigate, and respond promptly to cybersecurity incidents or events to ensure timely remediation.
6. Security Operation and Monitoring	The following managed security service features must be present in the bidder's solution: Security Operation Management 6.1 Establish a centralised SOC for 24/7 monitoring of security events and activities. 6.2 Develop and maintain a comprehensive cybersecurity strategy, including defined incident response procedures (IRP). 6.3 Implement and manage a Security Information and Event Management (SIEM) system to collect, correlate, and analyse logs across all environments. 6.4 Implement and manage Security Orchestration, Automation, and Response (SOAR) capabilities to automate threat detection, investigation, and response workflows. Threat Monitoring and Detection

	6.5 Provide ongoing monitoring of network, endpoints, and cloud environments to identify potential threats in real time. 6.6 Integrate external and internal threat intelligence feeds to detect emerging threats and vulnerabilities. 6.7 Use behavioural analytics and anomaly detection to identify suspicious activities indicative of potential security incidents. Incident Detection, Response and Management 6.8 Implement automated alerting and response mechanisms for detected security events to reduce response time. 6.9 Conduct thorough investigations of security events and breaches to determine cause, impact, and necessary remediation. 6.10 Document and report all security incidents, including lessons learned and remediation steps taken to prevent recurrence.
7. Data encryption	7.1 The service provider must implement and manage comprehensive encryption controls to ensure that all sensitive organisational data is protected both at rest and in transit. The current environment includes endpoint disk encryption (e.g., BitLocker). The bidder is required to enhance and extend encryption coverage across servers, endpoints, applications, backups, and data in transit in line with industry best practices. 7.2 The bidder must implement secure encryption key management processes and technologies, including key generation, storage, recovery and revocation. Key management must ensure that encryption keys can be securely recovered in the event of hardware failure or other critical incidents. 7.3 A bidder must establish a controlled and secure process for decrypting data when necessary, involving authorised personnel only and maintaining full auditability.
8. Advanced Electronic signatures (AES)	The bidder must provide a software solution that supports Advanced Electronic signatures (AES) for digitally signing final certificates for property valuations including business documents such as memos, policies and procedure. 8.1 The software must have the ability to convert PDF

	fields into signer fields and guide users to sign and initial in the correct locations. 8.2 Provide seamless integration with Active Directory, ERP systems, and Microsoft 365 applications to streamline workflows. 8.3 Ability to define customisable signing workflows that assign a specific number of signatories to different roles and control access. 8.4 Support multiple levels of authentication, including email-based, access code, and SMS verification to ensure signer identity. 8.5 Provide an electronic certificate with every signed document for verification and audit purposes. 8.6 Ensure all documents are digitally sealed using industry-standard technology, such as Public Key Infrastructure (PKI), to guarantee integrity and authenticity. 8.7 Ensure the software meets relevant regulatory standards such as Electronic Communications and Transaction Act (ECTA) for electronic signatures and document management.
9. Cyber security support	The bidder's solution must have the following managed security service features: 9.1 Support for incident detection. 9.2 Support for incident investigation. 9.3 Support for incident response. 9.4 Support in the recovery of incidents. 9.5 Review and support for adjustments following an incident.
10. Security assessment and penetration testing	The following managed security service requirements must be included in the bidder's solution 10.1 The bidder must conduct comprehensive security vulnerability assessments and penetration testing of the OVG's environment and infrastructure on a bi-annual basis. Testing must cover both internal (within OVG's network) and external (from outside/Internet-facing systems).
11. Monitoring dashboard	11.1 The bidder is required to provide the monitoring dashboard interface that is accessible internally within the OVG. 11.2 The dashboard must display live security monitoring feeds in Central Africa Time (CAT). 11.3 The monitoring dashboard must allow users to generate or draw reports as and when required. 11.4 The dashboard must include the ability to print reports directly.

	11.5 The supplied monitoring dashboard must be able to filter reports in (daily, weekly, monthly, ad hoc and calendar driven).
12. Security Management, Compliance, and reporting	The bidder's solution must provide comprehensive management, compliance, and reporting capabilities, including at minimum the following: 12.1 Provide monthly reports on all cybersecurity incidents and events that have transpired. 12.2 Provide monthly reports on all incidents and events that were investigated. 12.3 Gather and preserve possible digital evidence for cases involving administrative inquiries that may lead to civil investigations. 12.4 Provide status reports detailing remedial actions taken to address identified security issues. 12.5 Provide reports on cybersecurity risks, governance activities, and compliance status. 12.6 Report on occurrences and events monitored through the virtual SOC. 12.7 Ensure compliance with relevant industry and legal standards. 12.8 Provide a centralised management console for administrators to configure, monitor, and report on email security events. 12.9 Provide comprehensive audit trail reports to ensure accountability and traceability. 12.10 Provide SLA reports that track service performance against agreed targets. 12.11 Generate automated alerts. 12.12 Provide reports on vulnerability assessments and penetration testing conducted bi-annually.
13. Integration and Automation	13.1 The solution must support full integration and automation for SIEM and SOAR platforms.
14. Backup and Disaster recovery	14.1 The bidder must design, implement, and manage a comprehensive Disaster Recovery (DR) solution. The solution must include replication of the full production environment (physical and virtual servers, applications, and data) to a secure cloud to enable failover in the event of a disaster or major service disruption. 14.2 The bidder must implement and manage secure online backups of all data servers and critical data backup schedules; retention periods must be implemented in accordance with the OVG backup

	procedure. The estimated daily consumption of data is outlined in Annexure A. 14.3 The bidder must ensure seamless migration of archives and historical data from the current service provider into the new cloud DR environment. 14.4 The bidder must ensure that the cloud DR provides enterprise-grade resilience and high network availability. 14.5 The OVG requires that proposed cloud DR be hosted within the borders of South Africa. 14.6 The bidder must ensure that the cloud DR environment is secured through appropriate logical and network security controls, including firewalls, intrusion protection, secure connectivity, role-based access controls, and mandatory multi-factor authentication for all authorised users. Access to the DR environment must be restricted, monitored, and fully auditable. 14.7 The bidder must maintain policies and procedures that control access to cloud DR facilities and environments, including auditing and monitoring of all access attempts. 14.8 The bidder must guarantee the allocation of dedicated cloud resources for the OVG's workloads during recovery and disaster scenarios. 14.9 The solution must provide automated failover and failback processes, which will be executed during a disaster or service failure and completed within the Recovery Time Objective (RTO) and Recovery Point Objectives (RPO) as defined in the OVG's Business Continuity Management (BCM) Policy. 14.10 The bidder must provide sufficient bandwidth and scalable internet connectivity to support hosting and recovery of the OVG's systems in the cloud environment. 14.11 Where multi-tenant cloud infrastructure is shared with other clients, the bidder must conduct formal risk assessments, risk reduction reviews, and provide the OVG with details of residual risks that cannot be mitigated. 14.12 All Cloud DR services must comply with the OVG's Business Continuity Plan and meet required "Service Hours" for availability and responsiveness. 14.13 The successful bidder must provide regular Cloud DR training (at least twice a year) to relevant OVG staff, ensuring staff are equipped to support DR operations. Records of such training
--	---

	must be maintained. 14.14 In the event of significant changes to the Cloud DR environment, services, or recovery processes, the bidder must provide updated training to ensure OVG staff remain competent and informed. 14.15 The bidder, together with the OVG ICT staff, must conduct quarterly Cloud DR tests to validate recovery capabilities, especially when significant changes occur to the OVG requirements, workloads, or provider services. 14.16 The first Cloud DR test must be conducted within ninety (90) days of the first successful replication of the OVG's systems and data. 14.17 Disaster Recovery and backup restoration testing shall be conducted on a bi-annual basis to validate recovery procedures, data integrity, and system readiness. 14.18 The bidder must provide assurance that they have implemented robust business continuity and disaster recovery mechanisms for their own cloud infrastructure on which the OVG's systems and data are hosted. 14.19 The bidder must adhere to the OVG's Information Security policies and provide assurances that data and systems are not compromised in the cloud environment. 14.20 The bidder must ensure that the OVG's data is logically segregated from other client environments, with no cross-access or unauthorised disclosure permitted. 14.21 The bidder must ensure the confidentiality and integrity of the OVG's data during replication, transfer, storage, and recovery, in compliance with contractual obligations and data protection regulations (POPIA). 14.22 The bidder must demonstrate that all security incidents and weaknesses are promptly reported to the OVG and that corrective actions are taken in compliance with relevant security standards and frameworks equivalent incident management. 14.23 At the end of the contract, the bidder must guarantee that all the OVG data residing in their cloud environment is securely deleted, in compliance with relevant South African data protection and destruction laws, after providing OVG with a verified complete copy. (The service provider must provide the Certificate of Destruction as proof)
15. Cloud Security	15.2 The bidder's cloud environment must comply with

	internationally recognised standards and South African applicable legislation. 15.3 The bidder must maintain CSA STAR (Cloud Security Alliance Security, Trust, Assurance, and Risk) certification or demonstrate equivalent assurance through third-party audit reports (e.g., SOC 2 Type II). 15.4 The proposed cloud solution must include data encryption in transit and at rest, using industry-approved encryption algorithms (e.g., AES-256, TLS 1.3). 15.5 The bidder must ensure logical data segregation in multi-tenant environments to prevent unauthorized access or data leakage between clients. 15.6 The cloud platform must provide comprehensive identity and access controls, including multi-factor authentication (MFA) for administrative access, role-based access control (RBAC), and least privilege enforcement. 15.7 The bidder must have in place a documented Cloud Security Policy and Procedures aligned with security regulations, covering configuration management, vulnerability management, and security monitoring. 15.8 The bidder must maintain a cloud incident response plan compliant with recognised security standards and South African legislation, detailing processes for detection, containment, eradication, and recovery from cloud-specific incidents. 15.9 The bidder must ensure data residency within South Africa or provide legal and regulatory assurance that any cross-border data transfer complies fully with recognised security standards and South African legislation. 15.10 The bidder must provide the OVG with monthly cloud security posture reports, summarising: Identified and remediated, vulnerabilities, configuration changes, Security incidents or anomalies; and compliance status.
16. Training	The bidder must provide comprehensive cybersecurity awareness training for the OVG staff, including: 16.2 Bi-annual security awareness sessions to educate staff on cybersecurity best practices. 16.3 Regular updates and training materials to keep users informed of emerging threats.

	16.4 Attack simulations to test staff preparedness and reinforce learning through practical exercises. The bidder must provide a detailed Transfer of Skills plan for the OVG ICT personnel, covering at a minimum: 16.5 Methodology and approach for transferring knowledge and skills related to the implemented cybersecurity technologies. 16.6 Provide formal training on implemented technologies, including endpoint protection, email security, and other relevant systems.
--	--

4. CONTRACT MANAGEMENT

- 4.1 The bidder must provide a clear project plan with deliverables and timeframes. The bidder must clearly indicate the service availability times referring to the below business hours.

Table 3: Business Hours

Service Level	Business Hours	After Hours
	Monday - Friday 7:30am-4:00pm	Monday – Friday 4:00pm-7:30am and Weekends

- 4.2 The bidder must ensure that service is always available. Network issues, Loadshedding, engagements with other clients and any other interruption will not be accepted as reasons for not providing services.

5. TECHNICAL REQUIREMENTS

5.1 Licencing

- 5.1.1 The bidder is required to describe the license methodology or structure, explaining all the components within the managed security service offerings, including the pricing structure for related options and combinations. Bidders are required to list all the related components that should or could be part of the solution suite, whether they are relevant to the OVG's project.
- 5.1.2 The bidder must review the requirements and recommend the appropriate licensing model and associated costs to support the business requirements outlined in this TOR.
- 5.1.3 The license pricing must be based on a 'per use' and concurrent licensing model.

5.2 Support

- 5.2.1 Prospective bidders are required to provide a detailed support model.
- 5.2.2 Support is assumed to start immediately post-implementation.
- 5.2.3 Submit monthly SLA reports, weekly monitoring and system performance reports, and weekly escalated call log report.
- 5.2.4 Provide clear service level turn-around times with clear minimum resolution time per incident type. The minimum resolution times are as follows:

Table 4: Incident Response Timetable

Priority	Description	Minimum Time to Resolve
1	High Priority	4 hours
2	Medium Priority	8 hours
3	Low Priority	24 hours

5.3 Project Implementation Plan-Approach and Methodology

- 5.3.1 Bidders are required to submit a proposal covering a detailed implementation plan, the approach and implementation philosophy. This plan must cover allocated resources and timelines.
- 5.3.2 Failing to submit sufficient evidence may negatively impact your chances of being selected as the successful bidder.

6. AUTHORISED DELEGATE(S)

- 6.1 The scope of work may not be amended without the written confirmation of the Valuer-General or a duly delegated official.

7. SERVICE LEVEL AGREEMENT

- 7.1 The appointed bidder will have to enter into a service level agreement with the Office of the Valuer-General.
- 7.2 The appointed bidder must provide monthly service performance reports and participate in the periodic performance meetings.
- 7.3 Should the SLA not be finalized at the beginning of the services or within a period of 6 months, the Bidder shall not be relieved of its obligations to perform in terms of the appointment. In such circumstances, services and related meetings may commence and shall continue to be delivered in accordance with the Terms of Reference, the General Conditions of Contract, and all other applicable conditions, and contractual provisions issued in respect of this service.

Performance and compliance shall be monitored in terms of these documents until such time as the SLA is duly concluded and signed by both parties.

8. TENDERS WILL BE EVALUATED IN TERMS OF THE EVALUATION CRITERIA STIPULATED BELOW:

- a) Evaluation for mandatory criteria
- b) Evaluation in terms of Functionality
- c) Evaluation in terms of 80/20 preference point system as prescribed in the Preferential Procurement Regulations 2022

8.1 MANDATORY REQUIREMENTS

Bidder must comply with the requirements and submit all required document(s) indicated hereunder with the bid documents at the closing date and time of bid. This phase is not scored and bidder who fail to comply with all the mandatory criteria will be disqualified

Table 5:Mandatory Requirements

No	Mandatory Requirement	Substantiating Evidence of Compliance (Used to assess compliance)	Evidence Reference (To be completed by bidder)
	The Project Lead (Chief Information Security Officer) must provide at least one of the below mentioned senior-level internationally accredited and acceptable standard in cybersecurity certification as issued by a professionally accredited institution. Acceptable certifications include, but not limited to: • CISSP-Certified Information Systems Security Professional ((ISC²)) • CISM - Certified Information Security Manager (ISACA) • CCSP – Certified Cloud Security Professional (ISC²) NB: The bidder must ensure that the certificate is valid upon the award of the bid and OVG reserve the right to request valid certificate and verification of the authenticity will be done before award of the bid.	The bidder must submit proof of certification	Provide unique reference to locate substantiating evidence in the Bid response

	In the case of a Joint Venture (JV) , the submission must include a resolution from each participating company, as well as a joint resolution by the members of the Joint Venture authorising a designated member to sign all tender documents on behalf of the Joint Venture.		
	The Pricing Schedule (SBD 3.3 form) must be fully completed	Bidder is required to complete the Pricing Schedule (SBD 3.3) form and submit together with their Bid	Provide unique reference to locate substantiating evidence in the Bid response
	Attendance of the compulsory briefing session.	All the interested bidders are required to attend a compulsory briefing session	Attendance Register

8.2 ADMINISTRATIVE REQUIREMENTS

8.2.1 Tax Requirements:

- a) Bidder must ensure compliance with their tax obligations.
- b) Bidders are required to submit their unique personal identification number (pin) issued by SARS to enable the organ of state to view the taxpayer's profile and tax status.
- c) Application for tax compliance status (TCS) or pin may also be made via e-filing. To use this provision, taxpayers will need to register with SARS as e-filers through the website www.sars.gov.za.
- d) Bidder may also submit a printed TCS together with the bid.
- e) In bids where consortia / joint ventures / sub-contractors are involved; each party must submit a separate proof of TCS / pin / CSD number.
- f) Where no TCS is available, but the bidder is registered on the central supplier database (CSD), a CSD number must be provided.

8.2.2 Fully completion of SBD4 (Bidder's disclosure), SBD 6.1 (Preference Claim) & OVG supplier maintenance form

9. EVALUATION IN TERMS OF FUNCTIONALITY

- 9.1 Only the bidder who have complied with mandatory requirements will be evaluated for functionality. The bidder must, as part of their bid documents,

submit supporting documentation for all functional requirements as indicated here under. The Bid Evaluation Committee (BEC) responsible for scoring the respective bids will evaluate and score all bids based on their submissions and the information provided.

9.2 The value scored for each criterion will be multiplied with the specified weighting for the relevant criterion to obtain the marks scored for each criterion. These marks will be added and expressed as a fraction of the best possible score for all criteria.

9.3 Functionality will be evaluated based on the supporting documentation supplied by the bidder in accordance with the below functionality criteria and values.

9.4 The applicable values that will be utilised when scoring each criterion ranges from: 1 being Poor, 2 = Average 3 = Good, 4 = Very Good & 5 = Excellent.

9.5 The evaluation process will be conducted in **two Phases** as outlined below:

9.5.1 Phase 1: Technical/ Functional Evaluation

9.5.2 Phase 2: Physical Demonstration / Proof of Concept (POC)

Table 6: Phase 1 – Technical/Functional Evaluation

EVALUATION CRITERIA	GUIDELINES FOR CRITERIA APPLICATION	WEIGHT
COMPANY EXPERIENCE	Company experience: The bidder must demonstrate experience in supply, installation, configuration, support and monitoring of the Managed Security Services (MSS). The bidder must provide reference letters on a client letterhead. The letters must be signed, indicate the scope of work not more than five years and must have contactable references.	25
	Flexibility in customer service Provide a plan which includes service management approach, incident resolution times and response times.	5
TECHNICAL TEAM EXPERIENCE AND QUALIFICATION	Demonstrated knowledge and experience in the provision of implementing, designing, monitoring and managing security services and disaster recovery functions. The project team must have a minimum of NQF 6 qualification in IT related studies and security certificate.	
	CV TEMPLATE GUIDE	
	Employer	
	Position Held	
	Period	
	The name of the Employer including the client company if applicable	
	Provide the role description	
	Start Date	
	End Date	

	Responsibilities	Define the activities performed against this role.	
	Cloud Engineer		15
	Project Lead (CISO)		20
	Cyber Security Specialist		15
	NB: To substantiate maximum points in these criteria, bidders must follow the guide provided above when submitting Curriculum Vitae (CV) of the proposed Personnel.		
	NB: To substantiate maximum points in these criteria, bidders must attach the certificates and clearly indicate the role of the team member as outlined above.		
TECHNICAL APPROACH AND METHODOLOGY	Bidder must provide a comprehensive project methodology and execution plan that must at minimum cover time, cost, scope, resources, risk and quality inclusive of clear deliverables and timeframes for each task to be completed.		20
TOTAL POINTS ON FUNCTIONALITY MUST ADD TO 100			100

NB: No changes to the key resources are permitted without the prior written consent of the OVG, any replacement resources must have **equivalent or superior qualifications and experience** compared to the original team members evaluated. The original qualifications, experience, and professional body registrations (if applicable) formed the basis of the evaluation, and this standard must be maintained

Table 7:Phase 1 - Technical Evaluation Scoring Criteria

Scoring Criterion	1 Poor	2 Average	3 Good	4 Very Good	5 Excellent
Company Experience	1 reference letter of successfully completed project.	2 reference letters of successfully completed project.	3 reference letters of successfully completed projects.	4 reference letters of successfully completed projects.	5 and above reference letter of successfully completed project.
Flexibility in Customer Service	Inadequate Plan.	Plan that only addresses turnaroundtime over 8 hours.	Plan indicating turnaround time of 8 hours.	Plan indicating turnaround time of less than 6 hours.	Plan indicating turnaround time of 4 hours or less and any other interventions.
Cloud Engineer Experience	Less than 5 years of experience in implementing, designing, monitoring and managing cloud and disaster recovery services	5-6 years of experience in implementing, designing, monitoring and managing cloud and disaster recovery services.	7-9 years of experience in implementing, designing, monitoring and managing cloud and disaster recovery services	10-11 years of experience in implementing, designing, monitoring and managing cloud and disaster recovery services.	12 or more years of experience in implementing, designing, monitoring and managing cloud and disaster recovery services.
Cloud Engineer qualification	NQF 5 in IT related studies	NQF 6 in IT related studies	NQF 6 in IT related studies and one cloud certificate	NQF 6 in IT related studies and two cloud certificates	NQF 7 in IT related studies and two cloud certificates
Project Lead (CISO) Experience	0 - 4 years of experience in implementing, designing,	5 - 6 years of experience in implementing, designing,	7 – 9 years of experience in implementing, designing,	10 - 11 years of experience in implementing, designing,	12 or more years of experience in implementing, designing,

	monitoring and managing security services including leadership roles in similar projects.	monitoring and managing security services including leadership roles in similar projects.	monitoring and managing security services including leadership roles in similar projects.	monitoring and managing security services including leadership roles in similar projects.	monitoring and managing security services including leadership roles in similar projects.
Cybersecurity Specialist Experience	0 - 4 years of experience in implementing, designing, monitoring and managing security services.	5 - 6 years of experience in implementing, designing, monitoring and managing security services.	7 – 9 years of experience in implementing, designing, monitoring and managing security services, NQF 6 in IT related studies and one security certificate	10 - 11 years of experience in implementing, designing, monitoring and managing security services, NQF 6 in IT related studies and two security certificates	12 or more years of experience in implementing, designing, monitoring and managing security services, NQF 6 in IT related studies and two security certificates
Cybersecurity Specialist qualification	NQF 5 in IT related studies	NQF 6 in IT related studies	NQF 6 in IT related studies and one security certificate	NQF 6 in IT related studies and two security certificates	NQF 7 in IT related studies and two security certificates
Methodology	Inadequate Plan.		Plan that only partially addresses the scope of work.	Plan indicating scope of work, proposed work schedule/ duty sheet.	Plan indicating scope of work, proposed work schedule/ duty sheet/ work plan provided with clear deliverables.

Bids that fail to achieve a minimum of **60** points out of **100** points for technical evaluation will be disqualified. This means that such bids will not be evaluated on the second stage (Physical Demonstration/ Proof of Concept (POC)).

Table 8: Phase 2 - Physical Demonstration / Proof of Concept (POC)

EVALUATION CRITERIA	GUIDELINES FOR CRITERIA APPLICATION		WEIGHT
CYBERSECURITY SOLUTION	Bidders are required to provide a practical demonstration of the proposed security tools to confirm their capability, integration, and effectiveness in enhancing the organisation's overall security posture. The demonstration must address requirements as stated in Annexure B .		55
	Tool Description	Weight	
	Security Orchestration, Automation & Response (SOAR)	10 points	
	Security Incident & Event management (SIEM)	10 points	
	Identity and Access Management (IAM)	15 points	
	Email security Solution	10 points	
	Web application Firewall	5 points	
	Advanced Electronic Signature	5 points	

BACKUP AND DISASTER RECOVERY SOLUTION	The proposed solution must demonstrate the ability to ensure business continuity, data protection, and system availability in the event of system failures, cyber incidents, or disasters. The demonstration must address requirements as stated in Annexure C .	45
TOTAL POINTS ON FUNCTIONALITY MUST ADD TO 100		100

Table 9:Phase 2 - Physical Demonstration / Proof of Concept (POC) scoring criteria

Scoring Criterion	1 Poor	2 Average	3 Good
Security Orchestration, Automation & Response (SOAR)	The solution demonstrates only 1-2 functions of the System Requirement as indicated on Annexure B .	The solution demonstrates 3 functions of the System Requirement as indicated on Annexure B	The solution demonstrates between 4 to 7 functions of the System Requirement as indicated on Annexure B
Security Incident & Event management (SIEM)	The solution demonstrates only 1-2 functions of the System Requirement as indicated on Annexure B .	The solution demonstrates 3 functions of the System Requirement as indicated on Annexure B	The solution demonstrates between 4 to 9 functions of the System Requirement as indicated on Annexure B
Identity and Access Management (IAM)	The solution demonstrates only 1-2 functions of the System Requirement as indicated on Annexure B .	The solution demonstrates 3 functions of the System Requirement as indicated on Annexure B	The solution demonstrates between 4 to 7 functions of the System Requirement as indicated on Annexure B
Email security Solution	The solution demonstrates only 1-3 functions of the System Requirement as indicated on Annexure B .	The solution demonstrates 4 functions of the System Requirement as indicated on Annexure B	The solution demonstrates between 5 to 10 functions of the System Requirement as indicated on Annexure B
Web application Firewall	The solution demonstrates only 1-2 functions of the System Requirement as indicated on Annexure B .	The solution demonstrates 3 functions of the System Requirement as indicated on Annexure B	The solution demonstrates between 4 to 8 functions of the System Requirement as indicated on Annexure B
Advanced Electronic Signature	The solution demonstrates only 1-2 functions of the System Requirement as indicated on Annexure B .	The solution demonstrates 3 functions of the System Requirement as indicated on Annexure B	The solution demonstrates between 4 to 7 functions of the System Requirement as indicated on Annexure B
Backup and Disaster Recovery Solution	The solution demonstrates only 1-2 functions of the System Requirement as indicated on Annexure C .	The solution demonstrates 3 functions of the System Requirement as indicated on Annexure C	The solution demonstrates between 4 to 8 functions of the System Requirement as indicated on Annexure C

Bids that fail to achieve a minimum of **70** points out of **100** points for Physical Demonstration / Proof of Concept (POC) will be disqualified. This means that such bids will not be evaluated on the second stage (Preference Points System)

10. EVALUATION IN TERMS OF 80/20 PREFERENCE POINT SYSTEM

10.1 Only bids that achieve the minimum qualifying score for Physical Demonstration / Proof of Concept (POC) will be evaluated further in accordance with the 80/20 preference points system. Evaluation in this stage will be done as per the information furnished on the Pricing Schedule (SBD 3.3)

10.2 The 80/20 preference points system as prescribed in the Preferential Procurement Regulations, November 2022 pertaining to the Preferential Procurement Policy Framework Act, (ACT No 5 of 2000) (PPPFA) will be applied to evaluate this bid. The lowest acceptable bid will score 80 points for price, and a maximum of 20 points will be awarded according to the Specific Goal points claimable in respect of Preferential Status.

10.3 The following formula will be used to calculate the points out of 80 for price in respect of an invitation for a tender with a Rand value equal to or below R50 million, inclusive of all applicable taxes:

$$P_s = 80 \left(1 - \frac{P_t - P_{min}}{P_{min}} \right)$$

Where-

P_s = Points scored for price of tender under consideration. P_t = Price of tender under consideration; and

P_{min} = Price of lowest acceptable tender.

10.4 A maximum of 20 points may be awarded to a tenderer for the specific goal specified for the tender.

10.5 The points scored for the specific goal will be added to the points scored for price and the total will be rounded off to the nearest two decimal places.

10.6 Subject to section 2(1)(f) of the Act, the contract must be awarded to the tenderer scoring the highest points.

The specific goals allocated points in terms of this tender	Number of points allocated. (80/20 system)
Historically Disadvantaged individuals (HDIs)	
Who had no franchise in the elections before 1983 and 1993 Constitution	10
Who is a Female	5
People with Disabilities (PwDs)	5

- 10.7 Tenderers Preference points for HDI will be calculated on their percentage ownership or shareholding in business, if they are actively involved in and exercise control over the enterprise.
- 10.8 Where individuals are not actively involved in the management and daily business operations and do not exercise control over the enterprise commensurate with their degree of ownership, equity ownership may not be claimed.
- 10.9 A person awarded a contract because of preference for contracting with or providing equity ownership to an HDI, may not subcontract more than 25% of the value of the contract to a person who is not an HDI or does not qualify for the same number or more preference for equity ownership.
- 10.10 Preference points stipulated in respect of a tender must include preference points for equity ownership by HDIs. The equity ownership must be equated to the percentage of an enterprise or business owned by individuals or, in respect of a company, the percentage of a company's shares that are owned by individuals, who are actively involved in the management of the enterprise or business and exercise control over the enterprise, commensurate with their degree of ownership at the closing date of the tender.
- 10.11 If the percentage of ownership changes after the closing date of the tender, the tenderer must notify OVG and such tenderer will not be eligible for any preference points.
- 10.12 Preference points may not be claimed in respect of individuals who are not actively involved in the management of an enterprise or business and who do not exercise control over an enterprise or business commensurate with their degree of ownership.
- 10.13 All claims made for equity ownership by an HDI will be considered according to the following criteria:
- (i) Equity within private companies must be based on the percentage of equity ownership.
 - (ii) Preference points may not be awarded to public companies and tertiary institutions.
 - (iii) The following formula will be applied to calculate the number of points for equity ownership by an HDI:

$$NEP = \frac{NOP * EP}{100}$$

Where

NEP = Points awarded for equity ownership by an HDI

NOP= The maximum number of points awarded for equity ownership by an HDI

EP = The percentage of equity ownership by an HDI within the enterprise or business,

- 10.14 Equity claims for a Trust may only be allowed in respect of those persons who are both trustees and beneficiaries and who are actively involved in the management of the Trust.
- 10.15 Documentation to substantiate the validity of the credentials of the trustees must be submitted.
- 10.16 A Consortium or Joint Venture may, based on the percentage of the contract value managed or executed by their HDI members, be entitled to equity ownership in respect of an HDI.
- 10.17 The number of points scored for a Consortium or Joint Venture must be added to the number of points scored for achieving specified goals.
- 10.18 Bidders are required to submit proof of HDI. Proof includes valid Central Supplier Database (CSD) together with their tenders to substantiate their specific Goals claims for HDIs who had no franchise in the elections before 1983 and 1993 Constitution and Female.
- 10.19 Tenderers who do not submit proof of HDI claims as indicated above do not qualify for preference points for specific Goals but will not be disqualified from the tendering process.
- 10.20 CRITERIA FOR BREAKING DEADLOCK IN SCORING
- a) If two or more tenderers score an equal total number of points, the contract must be awarded to the tenderer that scored the highest points for specific goals.
 - b) If two or more tenderers score equal total points in all respects, the award must be decided by the drawing of lots.

11. REQUIREMENT FOR SUBMISSION OF THE PROPOSAL

- 11.1 Design a suitable methodology to undertake the assignment.
- 11.2 Submit a company profile that highlights capabilities relevant to MSS systems maintenance and support.
- 11.3 Demonstrate appropriate knowledge and experience in carrying out services of similar nature.
- 11.4 Attach full Curriculum Vitae of all the team members who are qualified and experienced in MSS systems maintenance and support.

- 11.5 Provide a Project Plan that outlines the Project life cycle.
- 11.6 Submit three recent references from organizations of which services of a similar magnitude have been successfully completed.
- 11.7 Bidders are advised to take note of the specified scope which will serve as a minimum performance matrix once the contract has been awarded. No changes to the scope will be entertained if the Bidder did not cost the services accordingly.

12. SECURITY AND CONFIDENTIALITY OF INFORMATION

- 12.1 No material or information derived from the provision of the services under the contract may be used for any other purpose except for those of the OVG, except where duly authorized to do so in writing by the OVG.
- 12.2 Copyright in respect of all documents and data prepared or developed for the purpose of the project by the Bidder shall be vested in OVG.
- 12.3 The successful Bidder agrees to keep confidential all records and information of or related to the project and not disclose such records or information to any third party or owner without the prior written consent of OVG.
- 12.4 The successful Bidder must undertake to disclose information relating to the contract only in terms of agreement entered and only to the parties stipulated in the contract, both during the contract period and subsequently. Information may only be disclosed to outside sources with prior written approval from the OVG.

13. MANAGEMENT OF THE PROJECT

- 13.1 The OVG will manage the project through the OVG PMO Framework. The responsible officials will manage implementation and monitoring of the bidder. The OVG assumes total accountability and therefore authorizes all expenditure for the project. All such expenses should be documented by the OVG.
- 13.2 Project Lead should issue out a completion/acceptance certificate for all deliverables.
- 13.3 The final contract will be based on the resources presented in the final accepted bid and any approved changes, making these resources a contractual obligation for the duration of the project.

14. TERMS AND CONDITIONS OF THE PROPOSAL

- 14.1 Awarding the proposal will be subject to the Bidder's expressing acceptance of the OVG Supply Chain Management Policy and the General Conditions of Contract as published by National Treasury.
- 14.2 The Bidder should not qualify the proposal with his/her own conditions. Any

qualification in the terms and conditions of this bid will result in disqualifications.

- 14.3 Any shortcoming in these terms of reference must be identified by the bidder prior to the awarding of a contract. Any shortcomings identified by the bidder after the contract has been awarded and that would have an impact on the contract price will be for the account of the bidder.
- 14.4 Should the bidder not comply with any of the conditions contained in these terms of reference during the contract period, the OVG may cancel the contract within one month's notice.
- 14.5 The pricing must be fixed for the duration of the contract.
- 14.6 The company and its employees will be subjected to positive security vetting and screening.
- 14.7 The Office of the Valuer-General shall:
- 14.7.1 Not accept responsibility/liability of accounts/ expenses incurred by the Bidder that was not agreed upon by the contracting parties.
- 14.7.2 Conduct business in a courteous and professional manner with the Bidder.
- 14.7.3 Not accept responsibility/liability of any damages suffered by the Bidder or the personnel for the duration of the project.
- 14.7.4 The OVG will enter into a Service Level Agreement upon appointment of the suitable Bidder. These TOR terms and Conditions will also form part of the contract.

15. REQUEST FOR FURTHER INFORMATION

All enquiries regarding the bid may be directed to the following:

Technical Enquiries

Overall general technical enquiries should be addressed to the following officials:

No.	Office	Contact person	Contact details
1	Office of the Valuer-General	Mrs J Modisamongwe	060 535 5778 012 036 0006 johannah.modisamongwe@ovg.org.za
2	Office of the Valuer-General	Ms M Maisa	081 037 0057 012 036 0004 mathabo.maisa@ovg.org.za

For supply chain management enquiries, please contact:

No.	Office	Contact person	Contact details
1	Office of the Valuer-General	Mr. G Sekwale	060 535 5769 012 036 0036 Gobusamang.Sekwale@ovg.org.za
2	Office of the Valuer-General	Ms. K Seatlholo	071 604 0399 012 036 0024 Kehilwe.seatlholo@ovg.org.za

16. ANNEXURES

ANNEXURES	Document
A. Daily backup consumption	Daily backup consumption.pdf
B. Security tools demonstration	Security Tools Requirements.pdf
C. DR and backup solution demonstration	Disaster Recovery and Backup Solution.pdf



Annexure A

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 any thing 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**
- 7.1 Within thirty (30) days of receipt of the notification of contract award,

security

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

- 16.1 The method and conditions of payment to be made to the supplier under this contract shall be specified in SCC.
- 16.2 The supplier shall furnish the purchaser with an invoice accompanied by a copy of the delivery note and upon fulfillment of other obligations stipulated in the contract.
- 16.3 Payments shall be made promptly by the purchaser, but in no case later than thirty (30) days after submission of an invoice or claim by the supplier.
- 16.4 Payment will be made in Rand unless otherwise stipulated in SCC.

17. Prices

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

18. Contract amendments

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

19. Assignment

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

20. Subcontracts

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

21. Delays in the supplier's performance

- 21.1 Delivery of the goods and performance of services shall be made by the supplier in accordance with the time schedule prescribed by the purchaser in the contract.
- 21.2 If at any time during performance of the contract, the supplier or its subcontractor(s) should encounter conditions impeding timely delivery of the goods and performance of services, the supplier shall promptly notify the purchaser in writing of the fact of the delay, its likely duration and its cause(s). As soon as practicable after receipt of the supplier's notice, the purchaser shall evaluate the situation and may at his discretion extend the supplier's time for performance, with or without the imposition of penalties, in which case the extension shall be ratified by the parties by amendment of contract.
- 21.3 No provision in a contract shall be deemed to prohibit the obtaining of supplies or services from a national department, provincial department, or a local authority.
- 21.4 The right is reserved to procure outside of the contract small quantities or to have minor essential services executed if an emergency arises, the supplier's point of supply is not situated at or near the place where the supplies are required, or the supplier's services are not readily

available.

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

21.6 Upon any delay beyond the delivery period in the case of a supplies contract, the purchaser shall, without 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 Programme (NIP)	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.