NATIONAL PROSECUTING AUTHORITY
South Africa

INVITATION TO BID

BID DETAILS

BID NUMBER	**:**	NPA 13-21/22
ISSUE DATE	**:**	
CLOSING DATE	**:**	6 December 2021
CLOSING TIME	**:**	11h00
DESCRIPTION	**:**	Firewall security refresh with Monitoring Tool, SIEM and DLP solution with five-year hardware and software maintenance and support.
MAINTENANCE CONTRACT	**:**	Five (5) years

COMPANY NAME **:** _____

CSD SUPPLIER NUMBER	UNIQUE REGISTRATION NUMBER

Please indicate whether this document is an original or copy, tick the applicable block.

ORIGINAL ☐ **COPY** ☐

SOFT COPY ☐

NB. AS PER NATIONAL TREASURY CIRCULAR, BIDDERS ARE REQUIRED TO REGISTER THEIR COMPANIES ON THE CENTRAL SUPPLIER DATABASE (CSD), SINCE SUPPLIERS WHO ARE NOT REGISTERED MAY NOT BE AWARDED BIDS WITH EFFECT FROM 01 JULY 2016. HTTPS://WWW.CSD.GOV.ZA

FULL DETAILS OF BIDDER

COMPANY NAME :_____

CONTACT PERSON : _____

DATE : _____

E-MAIL ADDRESS :_____

TELEPHONE NUMBER :_____

CELLULAR NUMBER :_____

FAX NUMBER :_____

PHYSICAL ADDRESS :_____

_____

_____

POSTAL ADDRESS :_____

_____

_____

SIGNATURE OF BIDDER :_____

DOCUMENTS CHECK LIST

Bidders are requested to use the checklist below for documents to be submitted with a bid.

NO	DOCUMENTS SUBMITTED	TICK (√)
1.	Proof of registration on a Central Supplier Database registration (CSD)	
2.	Certified Broad Based Black Economic Empowerment (B-BBEE) / Certificate or Original Sworn Affidavit confirming annual turnover and level of black ownership in case of an EME and QSE signed by the Commissioner of Oaths (SAPS).	
3.	Bidder's profile	
4.	Proposed methodology and schedule for project implementation plan, installation and configuration and maintenance plan as per **Section 3 Paragraph 39.2**	
5.	One (1) or more reference letters of previous clients indicating client satisfaction, contract duration, project description and bid amount as *per S***ection 3 Paragraph 39.4**	
6.	Certified copies of Identity Documents of Directors/Members/Shareholders/Trustees	
7.	Submit Curriculum Vitae's and Certificate(s) of experienced resources (Certified Engineers) on the equipment identified to be utilised for the duration of the contract.	
8.	One (1) original and Two (2) copies and optional USB of the bid document	
9.	Latest audited (where applicable) annual financial statements (not older than 18 months as at close of bid) as presented by an independent auditor or signed off by Accounting Officer in the case of Close Corporations.	
10.	A signed letter from the OEM certifying that the bidder is a partner or reseller.	

CONTENT PAGE

Bidders are to ensure that they receive all pages of this document, which consists of the following:

Structure of Proposals

Glossary

GLOSSARY

Award	Conclusion of the bid process and the final notification to the successful bidder
Bid	Written offer in a prescribed form in response to an invitation by NPA for the provision of goods, works or services
Briefing Session	A session that is held after the bid document is issued and before the closing date of the bid during which information is shared with potential bidders
Bidder	Organization with whom NPA will conclude a formal contract and potential Service Level Agreement subsequent to the final award of the contract based on this Request for Bid
Dti	Department of Trade and Industry
GCC	General Conditions of Contract
IP	Intellectual Property
NIPP	National Industrial Participation Programme
NPA	National Prosecuting Authority
Original Bid	Original document signed in ink
SCM	Supply Chain Management
SBD	Standard bidding document
SLA	Service Level Agreement
OEM	Original Equipment Manufacturer

SECTION 1 **SBD 1**

PART A

INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE NATIONAL PROSECUTING AUTHORITY					
BID NUMBER:	**NPA 13-21/22**	CLOSING DATE:	**6 DECEMBER 2021**	CLOSING TIME:	**11H00**
BID DESCRIPTION	Firewall security refresh with SIEM and DLP solution with five-year hardware and software maintenance and support for a period of five (5) years				

BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT *(STREET ADDRESS)*
National Prosecuting Authority
VGM Building Weavind Park
123 Westlake Avenue
Silverton
Pretoria

BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO		**TECHNICAL ENQUIRIES MAY BE DIRECTED TO:**	
CONTACT PERSON	**Thembi Ndleleni**	CONTACT PERSON	**Samuel Masombuka**
TELEPHONE NUMBER	**-**	TELEPHONE NUMBER	**-**
FACSIMILE NUMBER	**-**	FACSIMILE NUMBER	**-**
E-MAIL ADDRESS	**tenders@npa.gov.za**	E-MAIL ADDRESS	**tenders@npa.gov.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]			
1. ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	☐Yes ☐ No [IF YES ENCLOSE PROOF]	**2.** ARE YOU A FOREIGN BASED SUPPLIER FOR **THE GOODS /SERVICES /WORKS OFFERED?**	☐Yes ☐No [IF YES, ANSWER PART B:3]

QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS

IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)? ☐ YES ☐ NO

DOES THE ENTITY HAVE A BRANCH IN THE RSA? ☐ YES ☐ NO

DOES THE ENTITY HAVE A PERMANENT ESTABLISHMENT IN THE RSA? ☐ YES ☐ NO

DOES THE ENTITY HAVE ANY SOURCE OF INCOME IN THE RSA? ☐ YES ☐ NO

IS THE ENTITY LIABLE IN THE RSA FOR ANY FORM OF TAXATION? ☐ YES ☐ NO

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

PART B

TERMS AND CONDITIONS FOR BIDDING

1. BID SUBMISSION:

1.1. BIDS MUST BE DELIVERED BY THE STIPULATED TIME TO THE CORRECT ADDRESS. LATE BIDS WILL NOT BE ACCEPTED FOR CONSIDERATION.

1.2. **ALL BIDS MUST BE SUBMITTED ON THE OFFICIAL FORMS PROVIDED– (NOT TO BE RE-TYPED) OR IN THE MANNER PRESCRIBED IN THE BID DOCUMENT.**

1.3. THIS BID IS SUBJECT TO THE PREFERENTIAL PROCUREMENT POLICY FRAMEWORK ACT, 2000 AND THE PREFERENTIAL PROCUREMENT REGULATIONS, 2017, THE GENERAL CONDITIONS OF CONTRACT (GCC) AND, IF APPLICABLE, ANY OTHER SPECIAL CONDITIONS OF CONTRACT.

1.4. **THE SUCCESSFUL BIDDER WILL BE REQUIRED TO FILL IN AND SIGN A WRITTEN CONTRACT FORM (SBD7).**

2. TAX COMPLIANCE REQUIREMENTS

2.1 BIDDERS MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.

2.2 BIDDERS ARE REQUIRED TO SUBMIT THEIR UNIQUE PERSONAL IDENTIFICATION NUMBER (PIN) ISSUED BY SARS TO ENABLE THE ORGAN OF STATE TO VERIFY THE TAXPAYER'S PROFILE AND TAX STATUS.

2.3 APPLICATION FOR TAX COMPLIANCE STATUS (TCS) PIN MAY BE MADE VIA E-FILING THROUGH THE SARS WEBSITE WWW.SARS.GOV.ZA.

2.4 BIDDERS MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.

2.5 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED, EACH PARTY MUST SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.

2.6 WHERE NO TCS IS AVAILABLE BUT THE BIDDER IS REGISTERED ON THE CENTRAL SUPPLIER DATABASE (CSD), A CSD NUMBER MUST BE PROVIDED.

2.7 NO BIDS WILL BE CONSIDERED FROM PERSONS IN THE SERVICE OF THE STATE, COMPANIES WITH DIRECTORS WHO ARE PERSONS IN THE SERVICE OF THE STATE, OR CLOSE CORPORATIONS WITH MEMBERS PERSONS IN THE SERVICE OF THE STATE."

VALIDITY PERIOD: OFFER TO BE VALID FOR 90 DAYS FROM CLOSING DATE OF THE BID.

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

SIGNATURE OF BIDDER: ……

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

DATE:……...

SECTION 2

GENERAL CONDITIONS OF CONTRACT

THE GENERAL CONDITIONS OF THE CONTRACT WILL FORM PART OF ALL BID DOCUMENTS AND MAY NOT BE AMENDED

1. Definitions

1. The following terms shall be interpreted as indicated:

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

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

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

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

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

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

1.7 “Day” means calendar day.

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

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

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

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

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

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

1.14 “GCC” means the General Conditions of Contract.

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

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

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

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

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

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

1.21 “Purchaser” means the organization purchasing the goods.

1.22 “Republic” means the Republic of South Africa.

1.23 “SCC” means the Special Conditions of Contract.

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

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

2. Application

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

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

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

3. General

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

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

4. Standards

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

5. Use of contract documents and information; inspection.

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

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

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

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

6. Patent rights

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

7. Performance security

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

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.

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

22. Penalties

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

23. Termination for default

23.1 The purchaser, without prejudice to any other remedy for breach of contract, by written notice of default sent to the supplier, may terminate this contract in whole or in part:

(a) if the supplier fails to deliver any or all of the goods within the period(s) specified in the contract, or within any extension thereof granted by the purchaser pursuant to GCC Clause 21.2;

(b) if the Supplier fails to perform any other obligation(s) under the contract; or

(c) if the supplier, in the judgment of the purchaser, has engaged in corrupt or fraudulent practices in competing for or in executing the contract.

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

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

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

23.5 Any restriction imposed on any person by the Accounting Officer/Authority will, at the discretion of the Accounting Officer/Authority, also be applicable to any other enterprise or any partner, manager, director or other person who wholly or partly exercises or exercised or may exercise control over the enterprise of the first-mentioned person, and with which control over 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 office as contemplated in sections 12 and 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 endorse 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; an

(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

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

Participation Program (NIPP)

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 concerned.

SECTION 3

SPECIAL CONDITIONS OF CONTRACT

1. Bids submitted must be in line with the detailed specification. Failure to bid accordingly will result in the disqualification of the bids.

2. Bidders' attention is drawn to the fact that amendments to any of the Special Conditions will result in their bids being disqualified.

3. The NPA may, at any time or times prior to the bid submission date, issue to the bidders any amendment, annexure or addendum to bid documents. No amendment, annexure or addendum will form part of the bid documents unless it is in writing and expressly stated that it shall form part of the bid document.

4. The NPA reserves the right;

   - Not to appoint and/or cancel the bid at any time and shall not be bound to accept the lowest bid or proposal.
   - To award the bid as a whole or in part.
   - To enter into negotiation with one or more bidders regarding any terms and conditions, including price(s), of a proposed contract before or after the conclusion of the contract. (BAFO "Best and Final Offer")
   - To amend any bid condition, validity period, or extend the closing date of bids. Note: In terms of bid validity period extension, the bidder must respond within the required periods and in writing on whether or not he agrees to hold his original bid response valid under the same terms and conditions for a further period stipulated.
   - To conduct benchmarks on product/services offered during and after the evaluation.
   - To conduct a pre-award's survey during the source selection process to evaluate contractors' capabilities to meet the requirements specified in the bid and supporting documents.
   - To cancel and/or terminate the bid process at any stage, including after the closing date and/or after presentations have been made, and/or after bids have been evaluated and/or after shortlisted bidders have been notified of their status.
   - To conduct site inspections and or due diligence, or explanatory meetings in order to verify the nature and quality of services offered by the bidder. This will be done before/or after adjudication of the bid. The site inspection and or due diligence will be carried out with shortlisted bidders only.

5. The NPA may request written clarification or further information regarding any aspect of this bid. The bidders must supply the requested information in writing within two (2) working days after the request has been made, otherwise the proposal may be disqualified.
6. As per National Treasury Instruction, note no. 9 of 2017/2018, bidders are required to register their companies on the Government Central Supplier Database (CSD) and include in their bid a copy of

their Master Registration Number (Supplier Number) in order to enable the NPA to verify the bidder's tax status on Central Supplier Database.

7. Bidders are required to provide tax compliance status PIN or the Central Supplier Database Master Registration Number (MAAA Number) to enable the NPA to view their tax profile and verify the bidder's tax compliance status.

8. Foreign suppliers with neither South African tax obligation nor history of doing business in South Africa must complete a pre-award questionnaire on the Standard Bidding Document 1 for their tax obligation categorization.

9. Bidders are required to submit original and valid B-BBEE Status Level Verification Certificates or certified copies thereof or original sworn Affidavit signed by the Commissioner of Oath together with their bids, to substantiate their B-BBEE rating claims. In case of a trust, consortium or joint venture, a B-BBEE Status Level Verification Certificate must be submitted. Affidavits may only be commissioned by a person designated as a commissioner of Oaths In terms of Section 6 of the Justice of the Peace and Commissioners of Oaths Act, 1963-10 July 1998. *Copies of sworn affidavit will not be accepted*.

10. Bidders must submit documentary proof of the existence of joint ventures and/or consortium arrangements. The NPA will accept signed agreements as acceptable proof of the existence of a joint venture and/or consortium arrangement. The joint venture and/or consortium agreements must be clearly set out the roles and responsibilities of the Lead Partner and joint venture and/or consortium party. The agreement must also identify the Lead Partner, with the power of attorney to bind the other party/parties in respect of matters pertaining to the joint venture and/or consortium arrangement. Failure to adhere to the condition may lead to the bid being invalidated.

11. The principal bidder shall be responsible for the management of the contract. No separate contract shall be entered into between the NPA and any sub-contractors. Note: Copies of the signed agreements between the relevant parties must be attached to the proposal.

12. The NPA will enter into a Service Level Agreement with the successful bidder, effective from the date of bid award, taking all aspects of the contract into account.

13. Under no circumstances will negotiation with any bidders constitute an award or promise / undertaking to award the contract.

14. A bidder may not cede, assign or sub-contract any part of the assignment to any person unless with a written consent of the NPA and/or the court.

15. Bidders are requested to endorse their signature/initial on every page of the bid document. Furthermore, bidders must ensure that each place where a signature is required is correctly and fully signed including witnesses where applicable.

16. The NPA will not be liable for any expenses incurred by the bidders during the bidding process.
17. The bidder must have the infrastructure (physical premises) and the capacity to supply and/or deliver items/service required.

18. The employees of the bidder may be subject to screening for security purposes by the NPA at least once or as and when other surrounding circumstances so requires.

19. Any completion of bid documents in pencil, or the use of **correction fluid (Tippex), pencil or erasable ink** will not be acceptable and **will automatically disqualify the submitted bid**.

20. Preferential consideration will be given to bidders that are legal entities. In the case of sub-contracting or joint venture agreement, the NPA will enter into a single contract with a principal bidder.

21. A signed letter from the Original Equipment Manufacturer (OEM) certifying that the bidder is the accredited partner or reseller must be submitted with the proposal. **Failure to submit will result in disqualification.**

22. Service provider must take responsibility for any other third-party software (licencing) that is required for this solution.

23. All the required application security features must be licenced for the duration of this bid.

24. The NPA shall not accept any responsibility for expenses incurred by the service provider that was not agreed upon by the contracting parties.

25. The norms and quality of the services rendered, must be in accordance with the acceptable best practice.

26. The service provider may dispose of old firewall devices at a buy over cost as approved by the NPA. (No set-off cost against the new infrastructure will be allowed). If the service provider is not disposing of the old firewall devices, the NPA will follow its internal disposal process to handle the disposal of the old firewall devices.

27. The bidder shall ensure that the hardware to be provided has an on-site warranty for the duration of the contract.

28. Service provider to provide a firewall solution with Monitoring Tool, SIEM and DLP that will assist the NPA with its network defence in depth approach.

29. Service provider to migrate the current firewall configuration to the proposed firewall solution.

30. The NPA may at any given time add, combine, and/or remove offices from the list of offices, as listed in Section 6, Paragraph 12 (List of NPA office).

31. Payments in respect of a five (5) year maintenance and support will be made in monthly instalments for a duration of the contract.

32. The NPA will determine the usage of professional service hours. Unused hours will be claimed back by the NPA

33. Bidders must provide CV's and Certificate(s) of experienced resources (OEM Certified Engineers) that will be responsible for the maintenance and support services for the duration of the contract.

34. CONFLICT OF INTEREST, CORRUPTION AND FRAUD

34.1 The NPA reserves its right to disqualify any bidder who with or without their company / business, whether in respect of The NPA or any other government organ or entity and whether from the Republic of South Africa or otherwise ("Government Entity"), –

34.1.1 engages in any collusive tendering, anti-competitive conduct, or any other similar conduct, including but not limited to any collusion with any other Bidder or company / business in respect of the subject matter of this bid;

34.1.2 seeks any assistance, other than assistance officially provided by a Government Entity, from any employee, advisor or other representative of a Government Entity in order to obtain any unlawful advantage in relation to procurement or services provided or to be provided to a Government Entity;

34.1.3 makes or offers any gift, gratuity, anything of value or other inducement, whether lawful or unlawful, to any of The NPA's officers, directors, employees, advisors or other representatives;

34.1.4 accepts anything of value or an inducement that would or may provide financial gain, advantage or benefit in relation to procurement or services provided or to be provided to a Government Entity;

34.1.5 pays or agrees to pay to any person any fee, commission, percentage, brokerage fee, gift or any other consideration, that is contingent upon or results from the award of any tender, contract, right or entitlement which is in any way related to procurement or the rendering of any services to a Government Entity; or

34.1.6 has in the past engaged in any matter referred to above.

35 INDEMNITY

35.1 If a bidder breaches the conditions of this bid and, as a result of that breach, the NPA incurs costs or damages (including, without limitation, the cost of any investigations, procedural impairment, repetition of all or part of the bid process or enforcement of intellectual property rights / confidentiality obligations), then the bidder indemnifies and holds the NPA harmless from any and all such costs which the NPA may incur and for any damages or losses the NPA may suffer.

36 PRECEDENCE

36.1 This document will prevail over any information provided during any briefing session whether oral or written, unless such written information provided, expressly amends this document by reference.

37 TAX COMPLIANCE

37.1 No award shall be made to a bidder whose tax affairs are not in order. The NPA reserves the right to withdraw an award made to a bidder in the event that it is established that such bidder did not remain tax compliant for the full term of the contract.

38 GOVERNING LAW

38.1 South African law governs this bid and the bid response process. The Bidder agree to submit to the exclusive jurisdiction of the South African courts in any dispute of any kind that may arise out of or in connection with the subject matter of this bid, the bid itself and all processes associated with the bid.

39 THE BID PROPOSAL SHOULD INCLUDE BUT NOT LIMITED TO THE FOLLOWING IN DETAIL:

39.1 **Bidders profile –** A short summary and description of the key features of the bidder. The legal name of the entity, the principal business and if applicable an overview of the consortium with a description of the corporate organisation of the proposing entity including all the members of the consortia and/sub-contracts, if applicable the description and the role of the lead partner and participating companies of the consortium.

39.2 **Proposed methodology, project and implementation plan with timelines**- In this section, the bidder must demonstrate the understanding of the project indicating how its tasks and deliverables will be carried out, namely:

39.2.1 Provide a detailed project implementation plan with timelines, in order to ensure the solution is stable and adequately supported. Indicate how the project will be supported post the implementation phase.

39.2.2 Specify any other third-party software that is required for your solution to work that has not been included in your response.

39.2.3 Specify how installation and configuration of the firewall, DLP and SIEM solution would be achieved.

39.2.4 Network security professionals with relevant network security certification by OEM.

39.2.5 Maintenance (preventative and corrective) and support plan

39.3 **References and performance capabilities -** Bidders must provide information that demonstrates specific and/or adequate proof of related experience and performance capabilities in providing firewall service. Such claims must be supported with sufficient references to permit NPA to verify the claimed capabilities. To support all claims of experience presented and to assist the NPA in reviewing and evaluation of the proposals, the bidders are requested to provide the following**:**

39.3.1 One (1) or more signed reference letter(s) of previous clients where services required by this contract are/were offered, describing the services received, and the period of the contract i.e. Start and end Date of the contract in the last five years as well as

completing Section 13. (Note that the focus to these letters should address the relevant work experience of the bidder not the proposed approach to the requirement).

39.4 **Annual Financial Statements** - The bidder must provide an Annual Financial Statement (AFS) that is:

39.4.1 Not older than 18 months as at close of bid;

39.4.2 Audited (where applicable) annual financial statements or signed off by the Accounting Officer in the case of a Close Corporation.

SECTION 4

BID SUBMISSION REQUIREMENTS

1. WHO MAY SUBMIT A RESPONSE TO THIS BID?

1.1 NPA invites bids from bidders who comply with the requirements for this bid. In view of the scope of work required in this bid, the bidder must:

- Be able to deliver the scope and breadth of services as required.
- Comply with all other requirements as stipulated in the bid document.

2. FRAUD AND CORRUPTION

2.1 All service providers are to take note of the implications of contravening the Prevention and Combating of Corrupt Activities Act, Act No 12 of 2004 and any other Act applicable.

3. CLARIFICATION / QUERIES

3.1 Telephonic requests for clarification will not be considered. Any clarification required by a bidder regarding the meaning or interpretation of the Terms of Reference/specifications, or any other aspect concerning the bid or bid document, is to be requested in writing (letter, facsimile or e-mail) from the following contact person, stating the bid reference number:

Bid Enquiries : Thembi Ndleleni
E-mail : tenders@npa.gov.za

3.3 Queries received will be responded to within two (2) working days of receiving the query.

3.4 The NPA will not respond to any enquiries received less than seventy-two (72) hours before the closing date and time of the bid.

3.5 Bidders will get a copy of the bid document at the reception, **VGM Building (Corner Westlake & Hartley) 123 Westlake Avenue, Weavind Park, Silverton, Pretoria**, and the soft copy will be available on the NPA website (www.npa.gov.za) and the National Treasury e-tender Portal.

4. SUBMITTING BIDS

4.1 One (1) original plus two (2) copies and optional USB (soft copy) i.e. three (3) hard copies of bid proposals must be handed in / delivered to the address indicated below:

PHYSICAL ADDRESS	**COURIER / POSTAL ADDRESS**
NATIONAL PROSECUTING AUTHORITY **VGM BUILDING WEAVIND PARK** **123 WEST LAKE AVENUE** **SILVERTON** **PRETORIA**	**NATIONAL PROSECUTING AUTHORITY** **THE BID OFFICE** **PRIVATE BAG X 752** **PRETORIA** **0001**

4.2 It is the responsibility of the bidder to ensure that bid documents reach the NPA on or before the closing date and time of the bid on the addresses as outlined in paragraph 4.1 above. The NPA will NOT take responsibility for any bid documents received late.

NB: Bidders must indicate on the cover page of each document whether it is an original or a copy.

4.3 Should there be any bona fide discrepancy between the original document and the copy the original will be regarded as the valid document. Malicious discrepancies may result in the disqualification of the bidder.

4.4 All paper copies must be neatly bound. All additions to the bid document i.e. Appendices, supporting documentation, pamphlets, photographs, technical specifications and other support documentation covering the equipment offered etc. shall be neatly bound as part of the schedule concerned.

4.5 The NPA will not accept responsibility for any bid documentation, which gets lost.

4.6 An original version of the bid must be submitted. An authorized employee or representative of the bidder must sign the original version in ink, and each page of the proposal shall contain the initial of the same signatory/ies.

4.7 **Bulky documents**: Bidders are requested to arrange prior to submitting bulky documents. The NPA will not take responsibility for the bid documents left anywhere else other than the tender box as indicated in paragraph 4.1 above. Bidders are encouraged to call 012 845 7013/6077 or to email to tenders@npa.gov.za..

5. MARKING ON BID ENVELOPE / PACK

5.1 The proposals must be submitted in **a two (2) envelopes**. The objective of the exercise is to evaluate the Proposals Section without reference to the Price Section ensuring both sections are evaluated fairly and unbiased.

5.2 The **first (1st) envelope** holds all documents excluding the pricing proposal (schedule) and detailed supporting pricing documentation. **The second (2nd) envelope** holds the pricing schedule. An outer envelope encloses both envelopes that have the envelope addressing as stated in this document.

5.3 The NPA only opens the proposal – **the first envelope** – at the evaluation stage and only opens the pricing – **the second envelope** – for those bidders who met the predefined functionality threshold at the proposal evaluation.

5.4 Bids should be submitted in a sealed envelope, or sealed pack if too big for envelopes marked as follows:

- ❒ Attention : SCM Unit
- ❒ Bid number : NPA 13-21/22 (1st Envelope - **Functionality Proposal**)
  : NPA 13-21/22 (2nd Envelope – **Pricing Proposal**)
- ❒ Closing date and time : 6 December 2021 @ 11h00
- ❒ The name and address of the bidder:

5.5 It is the responsibility of the bidder to ensure that bid documents reach the NPA on or before the closing date of the bid on the addresses as outline on paragraph 4.1 above. The NPA will NOT take responsibility for any bid documents received late.

5.6 Documents submitted on time by bidders shall not be returned.

6. LATE BIDS

6.1. Bids received late shall not be considered. A bid will be considered late if it arrived even one second after 11:00am or any time thereafter. The tender (bid) box shall be locked at exactly 11:00am and bids arriving late will not be considered under any circumstances, such as traffic problems, getting lost etc. Bidders are

therefore strongly advised to ensure that bids are dispatched allowing enough time for any unforeseen events that may delay the delivery of bid.

6.2 The official Telkom time (Dial 1026) will be used to verify the exact closing time.

7. DIRECTIONS TO THE NPA OFFICES FOR DELIVERY OF BIDS

From Pretoria City Centre

Take the Pretoria Road (extension of Church Street East) leading to Silverton. Turn left (north) into Creswell Street opposite the Botanical Gardens. Proceed until you get to the second street and turn left into Hartley Street. Continue straight ahead, this will take you to the main entrance of the VGM building.

N1 from North

Take the Stormvoël turn-off. Turn left at the traffic light. At the next robot turn right into the street leading to Koedoespoort. Proceed through Koedoespoort over the 3-way stop. At the next street, turn right into Hartley Street which will lead you to the main entrance of the VGM Building.

N1 from South (coming from Johannesburg)

Take the Polokwane/Krugersdorp turn-off and follow the Polokwane N1 leading to the North. Proceed past Centurion and skip the following turn-offs: Botha Avenue, Alberton (old Jan Smuts), Rigel Avenue and Atterbury Road.

Take the Lynnwood Road turn-off and turn right into Lynnwood Road, over the highway and immediately left into Meiring Naude (direction CSIR). Pass the CSIR until you get to a T-junction with Cussonia Street. Turn left, keeping to the right side of the road. Take the curve right in front of the CBC School. At the second robot turn left into Creswell Road and at the second street thereafter turn left into Hartley Street. This will take you to the main entrance of the VGM Building. **Bidders should allow time to access the premises due to security arrangements that need to be observed.**

8. ACCESS TO INFORMATION

8.1 All bidders will be informed of the status of their bid once the bid process has been completed.

8.2 Requests for information regarding the bid process will be dealt with in line with the NPA SCM Policy and relevant legislation.

9. REASONS FOR REJECTION

9.1 NPA shall reject a proposal for the award of a contract if the recommended bidder has committed a proven corrupt or fraudulent act in competing for the particular contract.

9.2 NPA may disregard the bid of any bidder if that bidder, or any of its Directors:

9.2.1 Have abused the SCM system of NPA;
9.2.2 Have committed proven fraud or any other improper conduct in relation to such system;
9.2.3 Have failed to perform on any previous contract and the proof exists; such actions shall be communicated to the National Treasury.

9.3 Bidders that submit incomplete information and documentation not according to requirements of the terms of reference and special conditions.

9.4 Bidders that fail to submit proposal.
9.5 Bidders who receive information not available to other vendors through fraudulent means.

10. CANCELLATION OF BID PROCESS

10.1 The bid process can be postponed or cancelled at any stage provided such cancellation or postponement takes place prior to entering into a contract with a specific service provider to which the bid relates.

SECTION 5

EVALUATION AND SELECTION PROCESS

All bids received will be evaluated in accordance with the 80/20 preference system as prescribed in the Preferential Procurement Regulation of 2017. Evaluation process comprises of the following phases:

PHASE 1: **SCREENING PROCESS**

During this phase, bids will be reviewed to determine whether a bidder complied with all Standard Bidding documents, and whether a duly authorized representative signed such documents.

PHASE 2: MANDATORY REQUIREMENTS

Only bidders that have met the screening process will qualify for the mandatory requirements evaluation process. In this phase, the evaluation will be based on bidder's response in terms of compliance to the mandatory requirements.

1. Special instructions to Bidders

1.1 Bidders shall provide full and accurate responses in this document, explicitly state comply and provide reference regarding compliance. Bidders must substantiate their response, including full details on how their proposal/solution will address specific functional requirements and be adequately referenced.

1.2 If bidders do not comply fully with each of the mandatory requirements, the bid will be disqualified. No indication in the mandatory fields will be regarded as non-compliance.

2. Mandatory compliance requirements

2.1 Bidders must meet the following mandatory requirements. Bidders who do not meet all the following mandatory requirements will be disqualified from further evaluation.

FUNCTIONAL/ TECHNICAL EVALAUTION CRITERIA		
FUNCTIONAL REQUIREMENTS	**COMPLY**	**COMMENT/ REFERENCE**
Firewall Specification 1. **The Service Provider should provide:** 1.1. A firewall solution that will assist the NPA with its network defence in depth approach. 1.2. Migration of the current firewall configuration to the proposed firewall solution. 1.3. A detailed project implementation plan of how the proposed solution will be deployed to the NPA, 1.4. The service provider should submit a detail configuration plan on sign off of installation based on scope technical specifications.		
2. SLA Requirements 2.1. Critical component of the proposed solution is a comprehensive SLA for a five (5) year period that will include change and configuration management, as well as incident and event management 2.2. 24x7 Service Desk for single point of contact and escalations 2.3. Level 1 and Level 2 support from bidder. The support should be on-site. Includes support for day to day operational issues as and when these arise. 2.4. Level 3 and Level 4 support from OEM or the accredited service provider 2.5. Provide login to NPA for web access to OEM portal. 2.6. Monitored email support 2.7. Remote assistance using Remote Desktop and a Virtual Private Network (VPN) where available 2.8. Planned or Emergency Onsite assistance (extra costs apply) 2.9. Monthly system health check 2.10. License management 2.11. Hardware appliance guarantee		
3. Training – Accredited OEM Training 3.1. To provide complete technical training to three (3) NPA officials by the OEM or accredited service provider on behalf of the OEM on system design, configuration, operation, maintenance, management and administration of the system along with DNS setup, firewall appliances, appliance monitoring software, Security Information and Event Management (SIEM), Data Loss Protection (DLP), etc.		

TECHNICAL REQUIREMENTS	**COMPLY**	**COMMENT/ REFERENCE**
General Requirements 1. The firewall should support "Stateful" policy inspection technology. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc. 2. It should support the Firewall, IPSEC VPN & Bandwidth Management as integrated security functions. 3. The hardware platform & firewall with integrated IPSEC VPN application has to be from the same OEM. 4. The solution must include High Availability (HA). Appliance should support for Active –Active connections for HA requirements. 5. Licensing should be per device and not user/IP based (should support unlimited users). 6. Firewall should be supplied with the support for dynamic routing protocols, like RIP v2, OSPF, & BGP. 7. Firewall should support the multicast protocols as a multicast host, by participating in DVMRP, IGMP and PIMDM / PIM-SM. 8. Proposed Firewall OEM should be in the Leaders & Challengers Quadrant of Gartner Magic Quadrant for Enterprise Firewall. 9. Proposed Firewall must have an integrated IPS.		
Performance Requirements 1. Firewall Throughput (Large Packets) should be minimum of 10 Gbps. 2. Integrated IPS should be minimum of 3.5 Gbps. 3. The Firewall must support a minimum of 1 million concurrent connections. 4. The Firewall must support more than 50,000 new sessions per second processing. 5. Appliance should have a capability to support for more than 100 VLANs. 6. The appliance should have an internal storage capacity of minimum 128GB		

Network Protocols/Standards Support Requirements		
1. Network should support at least 200 protocols. 2. Firewall Modules should support the deployment in Routed as well as Transparent Mode. 3. The Firewall must provide state engine support for all common protocols of the TCP/IP stack. 4. The Firewall must provide NAT functionality, including dynamic and static NAT translations. 5. All internet-based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, and Ms-Exchange etc. 6. Local access to the firewall modules should support authentication protocols – RADIUS & TACACS+. 7. IPsec VPN should support the Authentication Header Protocols – MD5 & SHA. 8. IPsec encryption should be supported with 3DES, AES-128 & AES- 256 standards. 9. IPsec should have the functionality of PFS and NAT-T. 10. Firewall should support authentication proxy for Remote VPN, HTTP/HTTPS Applications Access, and various other applications 11. Firewall should support the authentication protocols RADIUS, LDAP, TACACS, and PKI methods. 12. Firewall should support PKI Authentication with PCKS#7 & PCKS#10 standards. 13. It should support BGP, OSPF, RIPv1 &2, Multicast Tunnels, DVMRP protocols. 14. Dynamic policy enforcement on VPN Clients.		

Firewall Filtering Requirements		
1. It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports.		
2. The Firewall must provide state engine support for all common protocols of the TCP/IP stack.		
3. The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type.		
4. The Firewall should be able to filter traffic even if the packets are fragmented.		
5. All internet-based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP, Lotus Notes, and Ms-Exchange etc.		
6. It should support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP and Skinny flows.		
7. It should be able to block Instant Messaging like Yahoo, MSN, and ICQ, Skype (SSL and HTTP tunnelled).		
8. It should enable blocking of Peer-Peer applications, like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP)		
9. The Firewall should support authentication protocols like LDAP,		
10. RADIUS and have support for firewall passwords, smart cards, & token-based products like Secured ID, LDAP-stored passwords, RADIUS or TACACS+ authentication servers, and X.509 digital certificates.		
11. The Firewall should support database related filtering and should have support for Oracle, MS-SQL, and Oracle SQL-Net.		
12. The Firewall should provide advanced NAT capabilities, supporting all applications and services-including H.323 and SIP based applications.		
13. Should support CLI & GUI based access to the firewall modules.		
14. Local access to firewall modules should support role-based access.		
15. QoS Support [Guaranteed bandwidth, Maximum bandwidth, Priority bandwidth utilization, QOS weighted priorities, QOS guarantee, QOS limits and QOS VPN].		

Integrated IPS Features 1. Integrated IPS functionality should be available as a module that can be activated and de-activated as and when required. 2. IPS should have the functionality of Software Fail Open. 3. IPS Software Fail Open functionality can be defined in terms of the Gateway Threshold of Memory or CPU and should have an option to trigger the mail if required. 4. The IPS should be constantly updated with new defences against emerging threats. 5. IPS updates should have an option of Automatic downloads and scheduling of updates for specific days and time. 6. Include flexibility to define newly downloaded protections to be set in Detect or Prevent mode. 7. Activation of new protections based on parameters similar to Performance impact, Confidence index, Threat severity etc. 8. IPS Engine should support Vulnerability and Exploit signatures, Protocol validation, Anomaly detection, Behaviour-based detection, Multi-element correlation. 9. IPS profile should be defined to Deactivate protections with Severity, Confidence level, Performance impact, Protocol Anomalies. 10. IPS Profile should have an option to select or re-select specific signatures that can be deactivated. 11. Intrusion Prevention should have an option to add exceptions for network and services 12. IPS should have the functionality to Block the traffic country wise. 13. IPS Policy to Block the traffic by country, should have an option to configure incoming direction, outgoing direction or both. 14. IPS events/protection exclusion rules can be created to view packet data directly from log entries with RAW Packets and if required can be sent to Wireshark for analysis. 15. Application Intelligence should have controls for Instant Messenger, Peer-to-Peer, Malware Traffic etc. 16. Instant Messenger should have options to Block File Transfer, Block Audio, Block Video, Application Sharing and Remote Assistance. 17. IPS should have an option to create own signatures with an open signature language. 18. IPS should provide detailed information on each protection, including: Vulnerability and threat descriptions, Threat severity, Performance impact, Release date, Industry Reference, Confidence level etc.		

Administration, Management and Logging 1. Firewall Real-Time Monitoring, Management & Log Collection (with storage) should not be distributed to more than ONE server/appliance. 2. Any changes or commands issued by an authenticated user should be logged to a database. 3. The firewall Management system should also provide real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, minimum of 6 million concurrent connections and a minimum of 250 000 connections/second counter. 4. The firewall must send mail or SNMP traps to Network Management Servers (NMS) in response to system failures or threshold violations of the health attributes. 5. The Firewall must provide simplified provisioning for addition of new firewalls whereby a standard firewall policy could be pushed into the new firewall. 6. The Firewall administration station must provide a means for exporting the firewall rules set and configuration. 7. Support for role-based administration of firewall. 8. The firewall administration software must provide a means of viewing, filtering and managing the log data. 9. The Firewall logs must contain information about the firewall policy rule that triggers a log. 10. The Firewall must provide minimum basic statistics about the health of the firewall and the amount of traffic traversing the firewall. 11. The Firewall should have Workflow functionality and an Audit for the Rule Change Management Process. 12. Management should have access to Visual Tracking of Changes in Policy, Detailed Summary Report of Changes carried out, Audit trails, Graphical comparison of Rule Base Changes and Session Management and Change approval process.		

DATA LOSS PROTECTION (DLP) SPECIFICATION

FUNCTIONAL/ TECHNICAL EVALAUTION CRITERIA		
FUNCTIONAL REQUIREMENTS	**COMPLY**	**COMMENT/ REFERENCE**
DLP Policy Enforcement **Detection - Fingerprinted Content** 1. Ability to fingerprint both structured (SSNs, CCNs, etc.) and unstructured data (MS Office docs, PDFs, CAD/CAM diagrams, source code, etc.) 2. Ability to fingerprint data using remote standalone tools that allow a secure and close-to-the-source indexing process 3. Ability to specify exactly which columns of fingerprinted structured data are needed to trigger a match (e.g., first name, last name, and SSN, but not ZIP) 4. Ability to specify certain combinations of columns of fingerprinted structured data that are NOT a match (e.g., first name and SSN without last name) 5. Ability to fingerprint structured data that contains multiple space-separated words (multi-token columns) 6. Ability to perform proportional proximity check for fingerprinted structured data. 7. Option to permit any or all data owners to send their own personal data (such as their own personal credit card number) outside the corporate network without violating a fingerprint rule. 8. For fingerprinted unstructured documents, ability to detect extracts or derivatives of these documents on a defined threshold percentage (e.g., register a match only if at least 30% of the document is matched) 9. Ability to normalize all common variants of data presentation (e.g., if data extract contains "123456789", it should match against "123-45-6789", "123456789", "123.45.6789", etc.) 10. Fingerprint large volumes of structured data (up to 6 billion cells of database information on a single detection server) 11. Fingerprint large number of unstructured documents (up to 2 million documents on a single detection server) 12. Support for exact and partial file content matching detection of fingerprinted unstructured at Endpoint level		

13. Ability to create template form libraries (for instance, tax, medical and finance forms) 14. Ability to recognize handwritten, electronically filled or machine generated data in template forms		
Detection - Learned Content 1. Detect unstructured documents of a particular type (proprietary source code, legal contracts, insurance claims, or other content types you specify) after using native machine-learning capabilities to analyse a small sample set. 2. Detect unstructured documents of a particular type without requiring fingerprints, while maintaining accuracy level comparable to fingerprinting. 3. Detect unstructured documents of a particular type using a lightweight index of document features that can be deployed to all products in the suite. Endpoint agent can accommodate this index while remaining compact and resource efficient. **4.** Detect new or never-before-seen unstructured documents of a particular type you specify		
Detection - Described Content 1. Detect on fully customizable lists of keywords and key phrases, with ability to include multiple keywords in a single detection rule and to specify keyword proximity required for a match 2. Detect against large keyword or key phrase lists (up to 100,000 keywords or key phrases) without performance degradation 3. Pre-built ability to detect a wide range of data patterns that represent confidential data (e.g., CCNs, BINs, magnetic stripe data, IBAN) 4. Pre-built ability to detect international identification or tax numbers. Countries include Argentina, Austria, Australia, Belgium, Brazil, Bulgaria, Canada, Chile, China, Czech Republic, Denmark, France, Germany, Greece, Hungary, Ireland, Israel, Italy, Luxemburg, Mexico, Netherlands, Norway, Poland, Romania, Russia, Singapore., South Africa, South Korea, Spain, Sweden, Switzerland, Taiwan, Thailand, United Arab Emirates, United Kingdom, Ukraine, United States, and Venezuela 5. Built-in intelligence about valid number ranges for different data types (e.g., only detecting SSNs assigned by Social Security Administration, only detecting CCNs passing a Luhn check) 6. Ability to automatically exclude invalid number ranges for specific data types (such as currently unassigned SSNs starting with numbers higher than 772)		

7. Ability to detect randomized RSA randomized social security numbers 8. Ability to create new data identification patterns with validators (for international ID numbers, proprietary bank account patterns, and so on) and to customize pre-built data identification patterns 9. Ability to check for the proximity of matched data identification patterns against a list of keywords 10. Detect based on fully customizable regular expressions 11. Detect based on file type (including encrypted, password-protected files, or unknown file-types), file name/extension, sender/recipient attributes, or transmission protocol 12. Detect based on extracted text from images using Optical Character Recognition in multiple languages 13. Detect based on metadata (tags, watermarks, etc.) 14. Ability to define custom file type signatures to detect file types that are not supported out-of-the-box 15. 60+ pre-built policy templates that include keywords and data patterns for U.S. and international regulations (e.g., HIPAA, PCI, GDPR) and corporate best practices that can easily be modified 16. Detect fingerprinted data in 25+ major South African languages, Western European and Asian languages (e.g., double-byte languages) 17. Detection relies on real-time content-aware detection, as opposed to "tagging" 18. Support natural language processing (NLP) for Chinese, Japanese, and Korean (CJK) keywords 19. Ability to create policies based on the number or size of attached files 20. Ability to extract and analyze information from files that are encrypted using Microsoft Rights Management Services (administered through Azure or Active Directory)		
Detection - Policy Definition 1. Ability to create a single policy in a single UI that can be deployed across all products (storage, network, endpoint, cloud) 2. All detection done on the distributed detection servers (or endpoint agents), not at the central management server 3. Configure policies to detect/set thresholds based on number of matches on a per-policy basis 4. Create policies that combine multiple detection technologies and rules with AND/OR logic and exception rules 5. Define group-based detection rules based on internal directory information, such as department or business unit 6. Ability to integrate directly with AD to create user- or group-based sender and recipient detection rules		

7. Ability to integrate directly with AD to create user- or group-based endpoint detection rules. Different policies can be applied based on logged-in user, even on a shared machine. 8. Ability to easily export/import existing policies, including policies, detection rules, profiles and other components from different systems (e.g. test to production) 9. Ability to define match thresholds based on unique matches of data identifier patterns 10. Ability to define match thresholds based on unique matches of keywords 11. Ability to define match thresholds based on unique matches of regular expressions 12. Ability to save and reuse sender and recipient rule patterns 13. Ability to download a detailed description of policies in a printer-friendly format, including the detection rules, exceptions, and response rules 14. Ability to clone existing policies		
Automated Enforcement 1. Automatically send customized email notifications to employee, employee's manager, and/or administrators 2. Automatically send message to a Syslog-enabled case management or security event management system 3. Configure multiple automated responses based on severity, match count, policy, etc. **4.** Ability to automatically assign incident status based on rule triggered and match count		
Role-Based Access and Privacy Control 1. Limit incident access for a role by policy, by department or business unit, by country or geography, by severity or remediation status, or by any user-defined custom attribute 2. Redaction of certain data such as sender identity information (email address, username, file owner, etc.) that may need to be kept confidential from certain users to protect employee privacy 3. Create separate roles for technical administration of servers, auditors, user administration, policy creation and editing, incident remediation, and incident viewing for data wherever it is stored or used, both on the network and on the endpoint 4. Ability to create roles based on granular Agent management tasks		
Incident Response Workflow 1. Fully customizable response interface allowing combinations of multiple remediation actions in a single UI action		

2. Individual work queues for members of incident response team(s) 3. Ability to (manually or automatically) assign per-incident data owners and to schedule automated sending of tailored incident lists to respective data owners 4. All relevant incident details on a single page to allow quick user decision-making and action 5. Per-user ability to customize the layout and data of the incident snapshot 6. "Match highlighting" showing specific sections of a message or file that violates policy 7. "Match highlighting" based on either minimum exposure or total number of existing matching tokens 8. Store and display in the UI the original message or file that generated the incident 9. Easily see how an incident is correlated to other incidents by subject, sender, recipient, filename, file owner, user name, and policy 10. View full incident history including all changes and edits to that incident 11. Sender, machine user, file owner identity resolution via LDAP and ability to integrate into non-LDAP sources of identity information to do things such as map an IP address back to a corporate user name/email 12. Ability to define custom incident attributes (e.g., department, business unit, sender contact information, incident cause, etc.) and populate either automatically from directory lookups or manually 13. Ability to export standalone HTML archive of incidents for external review by users without system access 14. Ability to have system pre-configured with settings optimized for specific industry verticals, including policies, reports, roles, and workflow		
Reporting and Analytics 1. Single user interface for all incidents (storage, network, endpoint, and cloud) as well as for systems management 2. Browser-based user interface accessible via Microsoft Edge browser 3. Per-user ability to view the user interface in English or South African language 4. Reporting of incidents and trends by organization, by department or by user utilizing enterprise directory 5. Multi-level summarization reports (e.g., incidents grouped by business unit, then by policy, and then by severity in the same report) 6. Ability to group, filter, and sort reports by different parameters, including department or business unit		

7. Configurable risk dashboards simultaneously showing different reports from storage, network, endpoint and cloud 8. Ability to configure and save custom reports and dashboards on a per-user basis 9. Option to publish saved reports to all users in a role or keep as private report 10. Ability to send any report via email, either on command or via regularly defined schedule 11. Capability to export reports to HTML, CSV, or XML format so they can be viewed outside the UI 12. Able to run reports on large incident databases (over 500,000 incidents) with minimal performance impact 13. Drill down on any report to get to addition incident detail without running a new report 14. Workflow aging reports providing incidents in different statuses, grouped by time period 15. Reporting API lets third-party applications extract incident data from, and update incidents in, the management console 16. Ability to generate views for programmatic access to incident data in the Data Loss Prevention database 17. Comprehensive list of standard system reports; ability to configure visible list of system reports by user 18. Ability to specify low-severity or remediated incidents as “archived," thereby excluding them from default incident reporting 19. Advanced reporting capabilities for multi-dimensional analysis (with robust graphical reporting features) across multiple DLP products and Enforce instances 20. Ability to define dashboards using dynamic Key Performance Indicators 21. Ad hoc reporting with pivot tables from a broad set of data, including incidents, repository scans, agent behavior, policy changes, and auditable actions 22. Provide insight into the behavior of specific individuals and focus on those users posing the highest risk		
Storage DLP - Target Coverage 1. Scan Windows file systems 2. Scan NAS filers such as NetApp filers 3. Scan relational databases (MS SQL Server, DB2, etc.) 4. Scan SharePoint 2014 or latest 5. Scan SharePoint Online 6. Scan SharePoint targets using claims-based, forms-based, or Windows authentication		

7. Scan Microsoft Exchange 2016 or latest 8. Scan Microsoft Exchange Online 9. Scan Microsoft .pst files with the ability to identify confidential data on a per message basis. 10. Scan encrypted repositories with the ability to decrypt and evaluate for policy matching. 11. Automatically locate servers and shares within a domain and produce a list that can be directly used as a file system target		
Storage DLP - Data Protection Actions 1. Automatically copy or relocate (quarantine) files which violate policy 2. Automatically quarantine (with option to manually release) confidential documents in SharePoint repositories. 3. Automatically collect files that match policy criteria for use in investigation or e-discovery request 4. Automatically remediate incidents if a previously detected incident does not appear in a subsequent scan 5. Automatic remediation can be performed based on item modification, detection policy changes or item existence 6. Leave customizable marker files in place of files that are relocated 7. Create customized responses for storage incidents 8. Un-quarantine or roll-back a relocated file to its original location 9. Apply digital rights to discovered confidential files including Microsoft MIP / AIP 10. Encrypt discovered confidential files in place with Encryption tools (may require 3rd party encryption tools to facilitate this requirement) 11. Ability to apply Encryption to CIFS File System server or Microsoft SharePoint scans. It can be using 3rd party encryption tools.		
Storage DLP - Actionable Incident Details 1. Display file location and owner information for files that violate policy 2. Display incident match details for files that violate policy 3. Offers method to identify file owners when the owner does not exist in the file system being scanned 4. Display file Access Control Lists (ACLs) for files that violate policy		
Storage DLP - Access Monitoring / Visualization and Risk Ranking (Data Insight) 1. Retrieve data about top general users of files that violate policy 2. Identify de facto file owner (most active user) even if file metadata is outdated, incomplete, or inaccurate		

5. Retrieve data about top users who have edited files that violate policy 6. Retrieve data about top readers of files that violate policy 7. Retrieve complete access history (for all users) on files that violate policy 8. User-friendly graphical and tabular representations of file usage 9. Provide user-friendly graphical representation of file-access audit logs 10. Retrieve list of all files a particular user has accessed in the past year (for user-focused investigation) 11. Retrieve Access Control Lists (ACLs) on directories 12. Retrieve information about the designated person responsible for remediating the specified files or folders (Custodian) 13. Display file-user and access data (top file users, complete access history, and so on) in storage incident snapshots 14. Scalable architecture that supports environments with up to 2 billion accesses annually 15. Visualization of effective, Windows, and NTFS-level permissions 16. Support for DFS 17. Support for NFS-based NetApp filers 18. Support for SharePoint 2014 or latest 19. Alert administrators on excessive file or folder access, with ability to white-list appropriate users 20. Identify outlier behaviour, such as file access by member of an AD group that doesn't typically access the file 21. Provide Folder Risk Reports that rank folders according to data loss risk (based on incident severity, folder openness, and user access) for the purposes of prioritizing remediation 22. Options for creating custom Folder Risk Reports, including ability to filter on various attributes (such as DLP policies, data owners, and folder location) and customize the risk-scoring formula 23. Designate one or more users as custodian for a filer, Web application, share, or folder (for remediation and reporting) 24. Flexibility to collect user and group information from heterogeneous directory services: Active Directory, LDAP, NIS, NIS+ 25. Ability to start rule-based scans according to last scan status: Failed, never scanned, or Partial. 26. Ability to use command line to run pre-built or ad hoc reports 27. Assess user entitlements governance for filers, SharePoint web applications, site collections and folders 28. Flexibility to define parameters used to determine whether a share's permissions are "open"		

29. Ability to distribute DLP remediation workflow directly to defined data owners or custodians and take incident remediation actions at file or folder level		
Storage DLP - Scan Management 1. Configure and control all scanning from a single, centralized console 2. Apply filters to only scan (or conversely ignore) files of a certain type or in a certain directory 3. Configure incremental scans in which only new or changed files are scanned 4. Apply filters to only scan files added, accessed, or modified in a certain date range 5. Preserve original file attributes including 'last accessed' attribute while scanning 6. Schedule automatically recurring scans 7. Ability to manually pause a scan 8. Configure windows of time when running scans will automatically pause (e.g., "pause scans during business hours") 9. Throttle scans to limit network bandwidth usage 10. Capable of performing quick inventory scans that complete when pre-defined incident count threshold is met 11. Capable of running multiple scans against multiple physical targets concurrently 12. Manage all scan target credentials on a single UI page, including applying a single credential to multiple targets 13. Ability to automatically discover and crawl open file shares on specified CIFS servers 14. Identify open file shares (on NAS devices) prior to scanning 15. Ability to distribute scans among multiple detection servers (grid scanning) 16. Ability to use the results of previous file system scans to speed up the scanning process		
Storage DLP - Scale and Security 1. Scan systems at remote locations with limited network bandwidth 2. Scan machines with agent-based or agentless deployment options 3. Supports storage scanning products running in a VMware image 4. Communications limited to fixed ports between target system and scanning server 5. No OS or software library requirements imposed on scanned system		

Endpoint DLP - Coverage 1. Agentless and agent-based scanning options 2. Agent-based discovery of confidential data on Windows and Mac endpoints (desktops/laptops), including reporting on Access Control Lists (ACLs) for files that violate policy 3. Agent offers full coverage when machine is on or off the corporate network (policies reside on the agent) 4. Agent stores incident-causing files in a cache until user reconnects to the corporate network		
Endpoint DLP - User Action Coverage 1. Monitor data downloaded to local drive 2. Monitor/block data copied to removable storage devices (USB, Firewire, SD, Thunderbolt on MAC, MTP on Windows 7 & 8, eSATA and compact flash cards) 3. Designate individual (or groups of) removable devices as trusted and create policy exceptions for those devices 4. Automatically encrypt confidential data upon copy to USB 5. Monitor/block data copied to CD/DVD 6. Monitor/block corporate email via Microsoft Outlook 7. Monitor/block HTTP transmissions 8. Monitor/block HTTPS transmissions via Microsoft Edge, Internet Explorer, Mozilla Firefox, Safari or Google Chrome 9. Monitor/block FTP transmissions 10. Monitor/block or exclude detection (by printer name) of data sent to local or networked printer 11. Monitor/block data sent to a local or networked fax 12. Monitor/block copy or paste actions 13. Monitor/block data copied to or from network file shares via Windows Explorer 14. Monitor/block data copied to network file shares from MAC clients 15. Monitor/block data copied through LAN Manager (LAN Man), Remote Desktop Protocol (RDP) and Web Distributed Authoring and Versioning (WebDAV) 16. Monitor/block use of confidential data by defined applications, including unauthorized encryption tools, IM programs and apps with proprietary protocols. Out-of-the-box coverage for Skype, Webex, LiveMeeting, Office Communicator, Bluetooth, iTunes, and Google Talk. 17. Monitor/blocks use of Outlook.com and Outlook Web App (OWA) 2007, 2010, 2013, and 2016 in both rich and light mode. 18. Monitor/blocks Microsoft Office 2013 file formats for detection and application monitoring, including the default formats for Microsoft		

Access, Excel, OneNote, Outlook, PowerPoint, Project, Publisher, and Word. 19. Monitor/block policy violations based on metadata 20. Cover endpoint actions performed through Citrix published applications and virtual desktops (using agents installed on Citrix server hosts only, not on endpoints) 21. Multi-vendor support for Virtual Desktop Infrastructure architectures, covering monitor storage volumes, print and fax requests, clipboards, and network activity on the virtual desktops. 22. Ability to monitor/block sensitive information uploaded through SharePoint using the Upload Multiple Files option 23. Monitor/block multiple file uploads to SharePoint using Windows Explorer drag and drop, and copy and paste 24. Support Clipboard copy and paste operations for Windows Store Mail app, Google Chrome, Microsoft Lync, Microsoft communicator and Skype on Windows endpoints 25. Support for monitoring and blocking save as operations from Microsoft Office applications (Word, Excel, and PowerPoint) to Box on Windows endpoints 26. Support for monitoring and blocking save operations from Outlook (versions 2019 and latest) using the Box for Office add-in 27. Support for monitoring Microsoft Teams and Jabber applications on Mac endpoints 28. Ability to define monitoring filters for copy to network shares from Mac and Windows endpoints and from network shares to Windows local drives 29. Ability to monitor System Integrity Protection (SIP) on Mac endpoints 30. Ability to apply Encryption to files copied to USB removable storage devices (May require integration with 3rd party encryption tools) 31. Support for monitoring and blocking files saved from Microsoft Office applications to OneDrive, SharePoint, and WebDav locations 32. Ability to control the level of access (blocked or read-only) to network shares and USB removable storage devices on Windows endpoints 33. Ability to enable or disable specific channels based on the agent location 34. Ability to prevent preventing printing Microsoft Office documents if they contain sensitive information, regardless of whether a particular printing job does not include the sensitive portion.		
Endpoint DLP - Agent Deployment and Management 1. Agent supported on: • Microsoft Windows Server 2016 & 2019 64-bit and latest. • Microsoft Windows 10 Enterprise 64-bit;		

2. Single agent performs all the functions including endpoint scanning and monitoring/blocking data leaving the endpoint 3. Set caps on % of CPU and disk, and amount of bandwidth used by agent for minimal impact on endpoint and network 4. Integrates with Windows OS drivers and various applications to ensure stability, interoperability, and security. Not a potentially destabilizing rootkit approach. 5. Deploy using standard systems management tools 6. Endpoint administration using a mature and dedicated agent management console 7. Target agent deployment by AD groups or Windows groups 8. Apply different agent configurations (covering different user actions, for example) to individual agents or groups of agents 9. Supports agent troubleshooting and diagnostic tools designed for non-IT users 10. Manage agent restart/shutdown, agent enable/disable, log retrieval, alerts, and configuration through central console 11. Point agent(s) to different Endpoint Server at any time, and configure agent(s) to fail over to secondary server if primary is not available 12. Additional options for centralized management of software deployment, software updates, and setting of logging levels 13. Dynamically apply policies and endpoint configurations based on agent properties, user or machine directory properties and conditions 14. Built-in Agent health status dashboard 15. Monitor and whitelist Windows Store applications 16. Centrally enable/disable the SPDY protocol on Internet Explorer and Firefox browsers 17. Ability to disable Print Screen / Shift Print Screen operations in supported Windows Operating Systems		
Endpoint DLP - Scalability 1. Agent-based scanning enables parallel scanning of thousands of endpoints 2. Ability to protect large volumes of data - entire database of customer records, large number of fingerprinted documents 3. Ability to support global distributed deployments of endpoint machines 4. Ability to support up to 30,000 endpoints per server 5. Ability to control Agent-Server connection interval and bandwidth throttle 6. Load-balancer and firewall friendly architecture to support Agents-Server communicating over public networks 7. Supports running server component of endpoint products in a VMware image		

Endpoint DLP - Agent Security 1. Out-of-the-box agent tamper-proofing protection 2. Agent does not appear in “Add/Remove Programs” and System Tray, and obfuscated in Services and Task Manager 3. Communications between agent and server are encrypted and authenticated 4. Option to require a password for agent uninstall 5. Agent-Server authentication based on standard protocols (HTTPS/certificates) 6. Ability to centrally define or change Endpoint Agent uninstallation and management passwords		
Endpoint DLP - Scan Management and Data Protection Actions 1. Same policies can be deployed to both agentless and agent-based scans 2. Configure and control all scanning from a single, centralized console 3. Configure incremental scans in which only new or changed files are scanned 4. Option to configure scan timeout by specifying maximum overall duration or maximum idle period 5. Agents report progress to a central location for up-to-date progress report while scans are running 6. Filter scans based on file size, type, location, and operating system environment variables 7. Ability for scan to run only when machine is idle, thus eliminating any adverse machine impact 8. Ability to quarantine confidential files locally (on endpoint) or to another network location 9. Ability to failover a secondary Endpoint Server for endpoint discover scan		
Endpoint DLP - Real Time Enforcement 1. On-screen, pop-up notification with hyperlinks and fields for user justification can appear upon the generation of an incident 2. Option for endpoint user self-remediation (on-screen notification prompting user to confirm whether to continue or cancel confidential data transfer) 3. Pop-up notification has automatic ability to present itself in one of 25+ languages based on underlying OS 4. Automatic email notification can be sent to user and/or manager upon the generation of an incident		

5. Enforce encryption of confidential files (with 3rd party Encryption tool) upon copy to removable devices such as USBs		
Network DLP - Multi-Protocol Monitoring Capabilities 1. Monitors any TCP-based protocol such as SMTP including attachments, HTTP including uploaded files, active and passive FTP including fully correlating transferred file data with control information 2. Monitors dual stack (IPv4 and IPv6) networks 3. Ability to monitor popular IM protocols and properly classify tunnelled IM traffic (HTTP) 4. Able to correlate IM traffic (native) for long-lived sessions 5. Can properly classify all protocols even when running on non-standard ports 6. Monitors gigabit speed lines without packet loss or requiring packet sampling to compensate for excessive load; does not require specialized NIC hardware 7. Ability to handle traffic bursts, buffer traffic, and provide insight into packets that cannot be processed 8. Ability to filter out network traffic for inspection based on protocol, IP range, or email sender/recipient email **9.** Provide detailed traffic statistics for overall data throughput, # of messages, and # of incidents on a per protocol basis and summarized down to an hourly level **10.** Ability to integrate with SSL visibility appliances to monitor encrypted traffic		
Network DLP - Multi-Protocol Prevention Capabilities 1. Conditionally block, reroute, or quarantine SMTP messages based on message content 2. Conditionally block HTTP messages based on message content 3. Conditionally remove content from HTTP posts to cloud and social networking sites (e.g., Facebook, Twitter, Salesforce.com) 4. Conditionally block encrypted web transmissions (HTTP over SSL) based on message content 5. Conditionally block FTP messages based on message content 6. Integrate with any SMTP-compliant MTA (e.g., Forcepoint email gateway, etc.) 7. Integrate with ICAP-enabled web proxies from Forcepoint web gateway 8. Ability to determine the username associated to a Web incident based on the dynamic correlation between IP addresses and Microsoft log on events		

9. Does not require use of embedded MTA or web proxy; can use existing or best-of-breed products 10. Integrate with email encryption gateways Forcepoint email gateway & Mimecast for content-aware conditional email encryption 11. Email blocking product can be deployed in either a reflecting (single MTA) or forwarding (multiple MTA) architecture 12. Email blocking product can inspect TLS-encrypted messages for secure communications with hosted/SaaS email providers (e.g., Forcepoint Email gateway. Cloud / Mimecast / Etc.) 13. Email blocking product can use DNS MX records to make forwarding decisions for better load balancing/failover 14. Supports integration with off-premises or hybrid cloud messaging and web security services infrastructure, including Mimecast Email Archiving, Google Apps, and Microsoft Online Services. 15. Handles conflicting policies by offering separate multi-policy handling rules 16. Automatic email notification can be sent to user and/or manager upon the generation of an incident 17. Supports network prevention products running in a Microsoft Hyper-V image 18. Provide remediation record of confidential email forwarded to supported encryption gateways 19. Closed-loop incident remediation for emails quarantined by supported MTAs		
Cloud DLP - Cloud email monitoring and protection 1. Ability to monitor corporate email sent from Microsoft Office 365 Exchange, Exchange Server 2016, and Google Enterprise Gmail with cloud-based detection infrastructure (Agentless) 2. Ability to block or modify emails containing confidential information sent from Microsoft Office 365 Exchange, Exchange Server 2016, and Google Enterprise Gmail leveraging cloud detection infrastructure (Agentless) 3. Ability to redirect Microsoft Office 365 Exchange, Exchange Server 2016, and Google Enterprise Gmail messages to email encryption gateways for secure delivery 4. Automatic real-time email notification can be sent to user, manager or other stakeholders after incident detection 5. Provide seamless integration with existing data loss prevention infrastructure, policies, incident remediation and workflow 6. Provide a cloud-based option for detection infrastructure 7. Ability to offer protection against targeted attacks, spear phishing, advanced malware, spam, and bulk mail as part as the cloud-based detection infrastructure		

Cloud DLP - Cloud Storage 1. Discover sensitive information stored in Box, Dropbox, SharePoint, Google Drive and OneDrive 2. Ability to report the stakeholders (including external parties) whom with employees have shared protected information 3. Ability to display which mechanisms are in use for sharing sensitive information, such as passwords or links requiring authentication 4. Identify sensitive information being openly exposed to unauthorized users 5. Ability to quarantine, release from quarantine, encrypt, or make a custom remediation of cloud storage incidents		
Cloud DLP - Enterprise file sync and share applications 1. Monitor and protect sensitive information from being uploaded/synched to cloud storage 2. Provide out-of-the-box as well as user-defined support to cloud storage applications		
Cloud DLP - Cloud Detection Service 1. Provide a managed REST detection service to enable third party integrations and partnerships 2. Provide "cloud-to-cloud" high performance detection service 3. Provide DLP Policy-driven response rules to third party vendors, such as cloud web security gateways and cloud application security brokers		
Cloud DLP - Cloud Application Security Broker 1. Ability to integrate with Cloud Application Security Broker via REST-based DLP cloud detection service to enable rich incident data and boost performance 2. Ability to target policies to specific cloud application security broker connectors 3. Ability to craft policy to detect multiple user interactions with files (for example, upload, download, share, move/copy, replace, etc.) 4. Ability to customize corrective user behavior (for example educate the user, notify manager, break public hyperlink, remove shares, quarantine, encrypt, block, etc.) 5. Ability to create policies based on CASB contextual attributes (i.e. User Threat Score, Location, Source Application, etc.) 6. Ability to invoke CASB remediation actions (dependant on CASB provider integration) 7. Provide closed-loop remediation for incidents solved in external cloud services (may require integration with 3rd party CASB provider)		

Cloud DLP - STANDALONE Cloud Based Console 1. Provide full cloud-based service for protecting Office 365 Exchange Online and Gmail for Work with no on-premises components 2. Ability to detect confidential information based on described content matching, including keyword, regex, and data identifier detection 3. Ability to detect confidential information based on file size and file type rules for attachments 4. Ability to detect a wide range of data patterns that represent confidential data (e.g., CCNs, BINs, magnetic stripe data, IBAN) 5. Include 60+ pre-built policy templates that include keywords and data patterns for U.S. and international regulations (e.g., HIPAA, PCI, GDPR) and corporate best practices that can easily be modified 6. Provide a comprehensive management platform for Data Loss Prevention violations 7. Provide automated and manual remediation workflow support, including email blocking, encryption, notifications, and data masking on detected violations 8. Integrate with SAML-based Identity Access Management systems 9. Support two-factor authentication 10. Support integration with Active Directory to enforce user- and group-based conditions		
DLP Platform - Distributed Architecture 1. Multi-tier architecture that scales to hundreds of detection servers and thousands of endpoint agents per server 2. High latency link tolerance for remote servers to enable remote location support over WANs, and server built-in self-recovery mechanisms to enable high availability 3. Automated software updates from centralized console to servers 4. Support for hybrid-cloud mode deployments relying on public IaaS providers for detection servers		
DLP Platform - System Management 1. System traffic, performance, and throughput metric reports 2. Enterprise-class database for high scalability, high performance and clustering support 3. Store multiple years of incident data in a centralized database (> 500,000 incidents) without data being discarded or overwritten 4. Flexible low-cost options to securely store incident attachments in a file system 5. Ability to delete incidents in bulk and purge specific incident details from database		

6. Built-in process to configure, schedule, start on demand, and monitor incident deletion jobs 7. Send real-time email alerts for system and server level conditions 8. Ability to support industry-standard x64 hardware and Windows & Linux operating system preferences 9. Customizable administrative Home Page based on user selection 10. Provide proactive pre-checker tools to validate database consistency prior to upgrades 11. Built-in database diagnostic modules 12. Built-in database space reclamation utilities 13. Provides search-based online Help experience, with access to the latest and most accurate content, including information from KB articles and user-forums.		
DLP Platform - System Access and Security 1. Supports Single Sign-On (SSO) using X.509 certificates for authentication. 2. Supports Security Assertion Markup Language (SAML)-based authentication using: Okta, SSO Circle. 3. Supports form-based, certificate-based, web-services-based, and Kerberos-based logon options using through SAML. 4. Data encrypted upon capture (monitors, discovery servers, agents) 5. Data stored in incident database in encrypted format 6. Communication channels between system components is authenticated and encrypted 7. All system passwords are encrypted including logon credentials for file scanning 8. All indexed data is protected even when created remotely (support of air-gap networks) 9. Detailed activity audit logs of database transactions and policy modifications 10. Hardened OS deployment model is supported with limited services and ports configurations		

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SPECIFICATION

FUNCTIONAL/ TECHNICAL EVALAUTION CRITERIA		
FUNCTIONAL REQUIREMENTS	**COMPLY**	**COMMENT/ REFERENCE**
Security Analytics 1. Provide continuously updated devices context, i.e., configuration, detection of installed software and patches and running services		

2. Should be able to Collect, Parse, Normalize, Index, and Store security logs at very high speeds 3. Detection of unauthorized network devices, applications, and configuration changes 4. Performance analytics on system and application along with contextual inter-relationship data for rapid triaging of security issues 5. Real-time user context, with audit trails of IP addresses, user identity changes 6. Capability to detect unauthorized network devices, applications, and configuration changes 7. Search historical events — e.g., Grouping by relevant aggregations, time of-day filters, regular expression matches		
Reporting and Incident Management 1. Capability to structure Incident reports to provide the highest priority to critical business services and applications 2. Should provide an interactive dashboard that visualizes collected data in the form of charts and graphs 3. Should allow to generate different types of reports. Reports are available in XML, HTML, and PDF. 4. To provide reports on security-related events and incidents. e.g., failed logins, malware activity, possible malicious activity, login attempts, etc. 5. Should Send alerts if an activity is detected as a potential security issue. For example, lateral movement. 6. Provide Sharable reports and analytics across organizations and users 7. Schedule reports and deliver results via email to key stakeholders 8. Capability to linking incidents to hosts, IPs and user to understand all related incidents quickly		
Configuration Change Monitoring 1. Capability to collect network configuration files, stored in a versioned repository 2. Capability to collect installed software versions 3. Automated detection of changes in network configuration and installed software 4. Automated detection of file/ folder changes 5. Provide Automated detection of changes from an approved configuration file. 6. Flexible user authentication local, external via Microsoft AD and Microsoft radius. 7. The solution must be compatible with Microsoft Server 2016 or latest, Exchange server 2016 or latest		

PHASE 3: FUNCTIONALITY EVALUATION

Only bidders that qualified on the mandatory requirements evaluation will be evaluated for functionality. At this phase, the evaluation process will be based on the bidder's response in respect of the bid proposal. Bidders who score a minimum qualifying score of 60% (percent) or more out of 100 on functionality will qualify to the next phase.

Functionality of the proposals will be evaluated on a scale of **0-5** in accordance with the criteria below. The rating will be as follows: 0=non-submission; 1=poor; 2=Average; 3=Good; 4= Very Good and 5= Excellent

EVALUATION CRITERIA	**WEIGHT**
1. Proposed Methodology	
Bidders must provide a detailed project implementation plan, demonstrating an understanding of the project, indicating how its tasks and deliverables shall be carried out, including timelines. The following should be indicated and highlighted on the proposal i.e. ▪ Provide a detailed project and implementation plan with timelines, in order to ensure the solution is stable and adequately supported. Indicate how the project will be supported post the implementation phase ▪ Specify how installation and configuration will be achieved ▪ Maintenance (preventative and corrective) and support plan	20 10 10
2. Experience and performance capabilities	
Bidders must demonstrate related experience and performance capabilities in providing firewall services, by providing documentary proof in the form of one or more reference letter(s) (on letter head of referee and signed by the relevant authority), confirming the period of the contract(s) where firewall services were conducted, indicating the start and end date of each contract. ▪ Up to One (1) year = 1 point ▪ Above one (1) year to two (2) years = 2 points ▪ Above two (2) to three (3) years = 3 points ▪ Above three (3) to four (4) years = 4 points ▪ Above four (4) years = 5 points Non-submission of reference letter(s) will score Zero (0) Points. Note: The focus of these letters should address the relevant wok experience of the bidder. This criterion will be evaluated in conjunction with section 13 (bidders experience)	30
3. Qualifications and skills of key personnel	
Bidders must provide CV's and Certificate(s) of experienced resources (OEM Certified Engineer(s)) that will be responsible for installation and configuration. ▪ From one (1) year to two (2) years = 2 points ▪ Above two (2) to three (3) years = 3 points ▪ Above three (3) to four (4) years = 4 points ▪ Above four (4) years = 5 points Failure to submit certificate(s) and CV's will score 0 points	20

EVALUATION CRITERIA	**WEIGHT**
4. Financial Stability	
Bidders must provide the latest audited (where applicable) annual financial statements (not older than 18 months as at close of bid) as presented by an independent auditor signed off by Accounting Officer in the case of Close Corporations. Point allocation will be based on the following revenue categories: ▪ R 7 million and above — 5 = points ▪ R 5 million to R 6,999,999 million — 4 = points ▪ R 3 million to R 4 999,999 million — 3 = points ▪ R 1 million to R 2,999,999 million — 2 = points ▪ R 999,999 to below — 1 = point ▪ Non-submission — 0 = point	10
Functional Total	**100**
Threshold	**60%**

The percentage for functionality will be calculated as follows:

$$Ps = \frac{so}{ms} \times 100$$

Where:
Ps = percentage scored for functionality by bid under consideration
So = total score of bid under consideration
Ms = maximum possible score, i.e. 5x (a) 100 = 500
Ap = percentage allocated for functionality (in this bid = 100)

i. The value scored for each criterion will be multiplied by the specified weight for the relevant criterion to obtain the marks scored for each criterion.
ii. The scores for each criterion will be added to obtain the total score.
iii. This score will be converted to a percentage and only bidders that have met or exceeded the minimum qualifying score of 60% on functionality will be evaluated and scored in terms of Price and B-BBEE status level contribution preference points.
iv. Bidders not meeting a minimum qualifying score of 60% on functionality will be disqualified.

PHASE 4: PRICE AND B-BBEE STATUS LEVEL CONTRIBUTION

Preference points claimed by bidders will be added to the points scored for price.

SECTION 6

TERMS OF REFERENCE: FIREWALL SECURITY REFRESH WITH SIEM AND DLP SOLUTION WITH FIVE (5) YEAR HARDWARE AND SOFTWARE MAINTENANCE AND SUPPORT.

1. Purpose

1.1 The NPA utilizes FortiGate firewalls as a solution. The devices were deployed to 32 NPA sites with ±3700 active users. The firewall security, SIEM and DLP are very critical to the business of the NPA, it ensures that NPA protects its network from unauthorized access and malicious attacks therefore facilitates the achievement of business continuity objectives of the organization. The NPA utilizes wireless access within its domain contributing to an integrated platform of ICT security.

1.2 It is anticipated that once the firewall security, SIEM and DLP infrastructure is implemented and a new maintenance and support contract is entered into, the organisation will be able to provide effective and stable ICT security, and provide critical network performance information that will enable effective infrastructure decision making.

1.3 Two additional security solutions, critically required to enhance the security posture in the organization, were identified. The previous solution didn't cater for SIEM and DLP. It was a standalone firewall solution.

1.4 The NPA offices are dispersed nationally with the Head Office at the VGM Building in Pretoria, being the nerve centre. The current firewall solution is deployed in all thirty-two (32) regional offices. These regional offices have localized datacentres that connect to the Head Office and SITA datacentre.

1.5 The NPA operating platform is primarily Microsoft (MS) Windows Server based 2012 R2/2016, MS Active Directory (AD) 2016, MS SQL 2014 and SharePoint 2014, MS CRM Dynamics 2013, and MS Exchange 2016. User desktop and laptop machines are installed with Windows 10 operating systems, MS Office 2019. All NPA offices have distributed architecture with decentralized datacentres.

1.6 Network Connectivity

1.6.1 The NPA uses Enterasys switch infrastructure for Local Area Network (LAN) connectivity.

1.6.2 The Wide Area Network (WAN) architecture resides on SITA's MPLS. Metro-E link make up the backbone of the SITA NGN.

1.6.3 Regional offices have Video Conference and Unified Communication solutions that are configured on the firewall.

2. PURPOSE OF THE BID

2.1 The purpose of this bid is to appoint a service provider to provide a firewall security refresh including a SIEM and DLP solution, inclusive of a five (5) year hardware and software maintenance and support service, to the NPA.

3. SCOPE OF WORK

3.1 Perform advanced planning for the deployment of the proposed solutions.
3.2 To provide a security gateway – installation and configuration of firewall appliances
3.3 To provide a security gateway - installation and configuration of SIEM and DLP solutions.
3.4 Manage internal and external access to resources for remote access or across the NPA network.
3.5 Manage and test VPN tunnels to allow greater monitoring and scalability.
3.6 Configure and maintain a secure and core acceleration solutions on the NPA network traffic, to ensure noted performance enhancement.
3.7 Licenses for Appliance Monitoring Software, Firewall, SIEM and DLP are all activated and remain active for the duration of 5 years.
3.8 Implementation of user identity awareness to troubleshoot user access issues at the NPA.
3.9 Service provider to provide a firewall solution with Monitoring Tool, SIEM and DLP that will assist the NPA with its network defence in-depth approach.
3.10 The implementation of the SIEM and DLP solution should include necessary infrastructure for the smooth operation of this solution.
3.11 The service provider should submit a detailed configuration plan document on sign-off of the installation based on the scope technical specification.
3.12 Handover after deployment with documentation of installation and configuration

4 Devices and/or software

4.1 31 Mid-Range Firewall appliances
4.2 4 High End Availability Core Firewall appliances
4.3 Appliance Monitoring Software
4.4 Security Information and Events Management (SIEM)
4.5 Data Loss Protection (DLP)

5 Maintenance and Support

5.1 On-site warranty: OEM warrantees.
5.1.1 On-site warranty: Standard factory OEM warranty

5.2 Five (5) years On-Site Services: Configuration, software and firmware upgrades and diagnoses.
5.2.1 Installation and configuration – Firewall, SIEM and DLP
5.2.2 Software and firmware upgrades
5.2.3 Network troubleshooting and health check
5.2.4 Break-fix and corrective maintenance
5.2.5 Preventative maintenance: Periodic proactive maintenance

5.3 Provide OEM Service Credits – These credits may be redeemed by the NPA for technical tasks related to the infrastructure.

5.4 Sign-off based on agreed acceptance criteria

5.5 Provide 24/7 hours available on call support.

6 240 Professional service hours (Certified Engineer/s) – services expected but not limited to:

6.1 Assisting with pro-active maintenance and architectural designs

6.2 Assisting NPA to manage, support and grow business

6.3 Provision of third and fourth level support from the OEM, in terms of the following:

- 6.3.1 Mid-Range Firewall appliances
- 6.3.2 High-end availability core Firewall appliances
- 6.3.3 Security Information and Event Management (SIEM)
- 6.3.4 Data Loss Protection (DLP)
- 6.3.5 Monitoring tool

7 Redundancy or Failover

7.1 Failover is required in the proposed architecture for the High-end availability core firewalls.

8 Disposal

8.1 The Service Provider may dispose of old firewall appliances at a buy over cost, as approved by the NPA. No set-off cost against the new infrastructure will be allowed.

8.2 If the Service Provider is not disposing of the old firewall appliances, the internal NPA disposal procedure will be followed to dispose of the old switches.

9 Training

9.1 Training of three (3) NPA Employees on Firewall, SIEM and DLP solutions

10 Project resources/certified engineers

10.1 **Certified Firewall, SIEM and DLP Expert**

- 10.1.1 Perform advance deployment configurations of the proposed solutions
- 10.1.2 Plan and deploy network security across all the NPA sites

10.2 **Certified Firewall, SIEM and DLP Admin**

- 10.2.1 Day to Day support and maintenance of the proposed solution.

11 Reporting

11.1 Provide monthly health check report

11.2 Compliance in terms of monthly vendor performance report

12 LIST OF NPA REGIONAL OFFICES

NAME OF THE REGION:	ADDRESSES
FREE STATE REGION	**Physical address**
DPP Bloemfontein	Waterfall Centre, C/o St Andrew & Aliwal Street, Bloemfontein
OWP Free State	Will be provided on request: confidential
EASTERN CAPE REGION	**Physical address**
DPP Grahamstown	Hayton Building, 94 High Street, Grahamstown, 6139
OWP Eastern Cape	Will be provided on request: confidential
DDPP Bhisho	Tourism House Building, Phalo Ave, Bhisho
DPP Mthatha	Broadcast House, c/o Sisson & Sutherland Street, Mthatha
DDPP East London	Spoornet Building, cnr Fleet & Station Street, East London
DDPP Port Elizabeth	18 Grahamstown Road, North End, Port Elizabeth
WESTERN CAPE REGION	**Physical address**
DPP Cape Town	NPA Building, 115 Leeuwen & Buitengracht Street, Cape Town
SCCU Cape Town	Commissioner House, Cnr AJ West & Voortrekker Streets, Bellville, Cape Town, Ground Floor
NORTHERN CAPE REGION	**Physical address**
DPP Kimberly	Wilcon House, 22 Fabricia Road, Beaconsfield, Kimberley
OWP Northern Cape	Will be provided on request: confidential
LIMPOPO REGION	**Physical address**
DPP Polokwane	High Court Building 1st Floor,36 Biccard Street, Polokwane
OWP LIMPOPO	Will be provided on request: confidential
DDPP Thohoyandou	Thohoyandou High Court, Mphehphu Drive Thohoyandou
MPUMALANGA REGION	**Physical address**
DPP Nelspruit	Mpumalanga Division of the High Court, Cnr Samora Machel and Kaapse Hoop Road, Mbombela
OWP Mpumalanga	Will be provided on request: confidential
NORTH WEST REGION	

DPP Mmabatho	Megacity Building 2nd and 3rd Floor, East Gallery, Sekame Street, Mafikeng
OWP North West	Will be provided on request: confidential
KZN REGION	
DPP Pietermaritzburg	313 Pietermaritz Street, Pietermaritzburg
DDPP Durban	Southern Life Building, 88 Joe Slovo Street, Durban
OWP KZN	Will be provided on request: confidential
SSCU Durban	John Ross House, Victoria Embankment, Durban, 6th Floor
GAUTENG REGION	**Physical address**
DPP JHB	Innes Chambers, 51 Pritchard Street, Johannesburg
Investigating Directorate (ID)	Brooklyn Bridge, Linton House, Building no 5, 570 Fehrsen Street, Nieuw Muckleneuck (Brooklyn), Pretoria
NPA HQ:	VGM Building, 123 Westlake Avenue, Weavind Park, Pretoria
SITA Centurion	Sita Centre,459 John Vorster Drive, Centurion
DPP Pretoria	28 Church Square, Pretoria
SCCU Pretoria	7th Floor, 228 Visagie Street, Pretoria
OWP Gauteng	Will be provided on request: confidential

SECTION 7

PRICING SCHEDULE- (FIXED PRICES)

NAME OF BIDDER: …..…….…..… **BID NO.: NPA 13-21/22**
CLOSING DATE: 6 DECEMBER 2021 **CLOSING TIME: 11H00**

1. Bidders are required to indicate a total bid price based on the total requirements of the contract and including **all expenses** inclusive of VAT for the project.

Items & description	**Item Description**	**Total price (Including VAT)**
Firewall Devices	Firewall Appliances ***(including five (5) year on-site warranty)*** ▪ 31 Mid-Range dedicated hardware security devices. ▪ 4 High End availability core device	R
DLP Solution	Appliances ***(including five (5) year on-site warranty)***	R
SIEM Solution	Appliances ***(including five (5) year on-site warranty)***	R
Monitoring tool	Device Monitoring services	R
Professional Services	240 Hour services	R
Once off implementation services		R
Once off training for three (3) NPA resources		R
Five (5) years licenses for Monitoring Tool, Firewall, SIEM & DLP		
Year 1		R
Year 2		R
Year 3		R
Year 4		R
Year 5		R
Five (5) years maintenance and support for Monitoring Tool, Firewall, SIEM & DLP		
Year 1		R
Year 2		R
Year 3		R
Year 4		R
Year 5		R
TOTAL AMOUNT		**R**

2. FIVE (5) YEARS MAINTENANCE AND SUPPORT CONTRACT

1. Bidders are required to indicate a five (5) years maintenance and support amount on the above pricing schedule. (**Note:** Prices accepted must remain fixed and firm from the date of acceptance for a contract period of five (5) years. Any possible price increases and/or escalations must be considered because no additional costs will be admitted later).

2. Maintenance and support services will be paid on an accrual basis once the services has been rendered.

3. IMPORTED ITEM(S)

3.1 Bidders are required to keep their bid price fixed for imported items for a period of 90 days and thereafter Rate of Exchange (RoE) will be considered.

4. CONDITIONS APPLICABLE TO THE BIDDER'S PRICING

4.1 The bidders must complete the pricing schedule (inclusive of any escalation and/or all costs deemed necessary as no additional costs will be admitted later on non-imported items).

4.2 Rates must be quoted in South African Rands and must be inclusive of all applicable taxes.

4.3 Prices are to remain fixed and valid. Non-fixed prices will not be considered except for imported items. Failure to provide fixed prices will result in disqualification.

NOTE: Bidders are required to complete the above pricing schedule in full. Prices including more than one item or combined together must be indicated as such.

Declaration

I/We have examined the information and conditions provided in pricing schedule. I/We confirm that the prices quoted in this bid are fixed and valid for the stipulated period.

Signature of bidder: .....

Date: .....

SECTION 8

SBD 6.1

PREFERENCE POINTS CLAIM FORM IN TERMS OF THE PREFERENTIAL PROCUREMENT REGULATIONS 2017

This preference form must form part of all bids invited. It contains general information and serves as a claim form for preference points for Broad-Based Black Economic Empowerment (B-BBEE) Status Level of Contribution

NB: BEFORE COMPLETING THIS FORM, BIDDERS MUST STUDY THE GENERAL CONDITIONS, DEFINITIONS AND DIRECTIVES APPLICABLE IN RESPECT OF B-BBEE, AS PRESCRIBED IN THE PREFERENTIAL PROCUREMENT REGULATIONS, 2017.

---

1. GENERAL CONDITIONS

1.1 The following preference point systems are applicable to all bids:

- 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

a) The value of this bid is estimated to not exceed R50 000 000 (all applicable taxes included) and therefore the 80/20 preference point system shall be applicable; or

b) Points for this bid shall be awarded for:

(a) Price; and

(b) B-BBEE Status Level of Contributor.

1.3 The maximum points for this bid are allocated as follows:

	POINTS
PRICE	80
B-BBEE STATUS LEVEL OF CONTRIBUTOR	20
TOTAL POINTS FOR PRICE AND B-BBEE MUST NOT EXCEED	**100**

1.4 Failure on the part of a bidder to submit proof of B-BBEE Status level of contributor together with the bid, will be interpreted to mean that preference points for B-BBEE status level of contribution are not claimed.

1.5 The purchaser reserves the right to require of a bidder, either before a bid is adjudicated or at any time subsequently, to substantiate any claim in regard to preferences, in any manner required by the purchaser.

2. DEFINITIONS

(a) **"B-BBEE"** means broad-based black economic empowerment as defined in section 1 of the Broad-Based Black Economic Empowerment Act;

(b) "**B-BBEE status level of contributor"** means the B-BBEE status of an entity in terms of a code of good practice on black economic empowerment, issued in terms of section 9(1) of

the Broad-Based Black Economic Empowerment Act;

(c) **"bid"** means a written offer in a prescribed or stipulated form in response to an invitation by an organ of state for the provision of goods or services, through price quotations, advertised competitive bidding processes or proposals;

(d) **"Broad-Based Black Economic Empowerment Act"** means the Broad-Based Black Economic Empowerment Act, 2003 (Act No. 53 of 2003);

(e) **"EME"** means an Exempted Micro Enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;

(f) **"functionality"** means the ability of a tenderer to provide goods or services in accordance with specifications as set out in the tender documents.

(g) **"prices"** includes all applicable taxes less all unconditional discounts;

(h) **"proof of B-BBEE status level of contributor"** means:

1. B-BBEE Status level certificate issued by an authorized body or person;
2. A sworn affidavit as prescribed by the B-BBEE Codes of Good Practice;
3. Any other requirement prescribed in terms of the B-BBEE Act;

(i) **"QSE"** means a qualifying small business enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;

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

POINTS AWARDED FOR PRICE

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

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

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

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

Where

Ps = Points scored for price of bid under consideration

Pt = Price of bid under consideration

Pmin = Price of lowest acceptable bid

4. POINTS AWARDED FOR B-BBEE STATUS LEVEL OF CONTRIBUTOR

4.1 In terms of Regulation 6 (2) and 7 (2) of the Preferential Procurement Regulations, preference points must be awarded to a bidder for attaining the B-BBEE status level of contribution in accordance with the table below:

B-BBEE Status Level of Contributor	Number of points (90/10 system)	Number of points (80/20 system)
1	10	20
2	9	18
3	6	14
4	5	12
5	4	8
6	3	6
7	2	4
8	1	2
Non-compliant contributor	0	0

5. BID DECLARATION

5.1 Bidders who claim points in respect of B-BBEE Status Level of Contribution must complete the following:

6. B-BBEE STATUS LEVEL OF CONTRIBUTOR CLAIMED IN TERMS OF PARAGRAPHS 1.4 AND 4.1

6.1 B-BBEE Status Level of Contributor: . = ……(maximum of 10 or 20 points)

(Points claimed in respect of paragraph 7.1 must be in accordance with the table reflected in paragraph 4.1 and must be substantiated by relevant proof of B-BBEE status level of contributor.

7. SUB-CONTRACTING

7.1 Will any portion of the contract be sub-contracted?

(***Tick applicable box***)

YES		NO	

7.1.1 If yes, indicate:

i) What percentage of the contract will be subcontracted.....……%
ii) The name of the sub-contractor……..
iii) The B-BBEE status level of the sub-contractor.....……..
iv) Whether the sub-contractor is an EME or QSE
(Tick applicable box)

YES		NO	

v) Specify, by ticking the appropriate box, if subcontracting with an enterprise in terms of Preferential Procurement Regulations, 2017:

Designated Group: An EME or QSE which is at last 51% owned by:	**EME** √	**QSE** √
Black people		
Black people who are youth		
Black people who are women		
Black people with disabilities		
Black people living in rural or underdeveloped areas or townships		
Cooperative owned by black people		
Black people who are military veterans		
OR		
Any EME		
Any QSE		

8. **DECLARATION WITH REGARD TO COMPANY/FIRM**

8.1 Name of company/firm:…….

8.2 VAT registration number:……..……

8.3 Company registration number:…….……

8.4 TYPE OF COMPANY/ FIRM

- □ Partnership/Joint Venture / Consortium
- □ One person business/sole propriety
- □ Close corporation
- □ Company
- □ (Pty) Limited

[TICK APPLICABLE BOX]

8.5 DESCRIBE PRINCIPAL BUSINESS ACTIVITIES

……
……
……
……..

8.6 COMPANY CLASSIFICATION

- □ Manufacturer
- □ Supplier
- □ Professional service provider
- □ Other service providers, e.g. transporter, etc.

[*TICK APPLICABLE BOX*]

8.7 Total number of years the company/firm has been in business:……

8.8 I/we, the undersigned, who is / are duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the B-BBE status level of contributor indicated in paragraphs 1.4 and 6.1 of the foregoing certificate, qualifies the company/ firm for the preference(s) shown and I / we 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 6.1, the contractor may be required to furnish documentary proof to the satisfaction of the purchaser that the claims are correct;

iv) If the B-BBEE status level of contributor has been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the purchaser may, in addition to any other remedy it may have –

(a) disqualify the person from the bidding 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 bidder or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted by the National Treasury 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.

WITNESSES 1. …….. 2. …….	…… SIGNATURE(S) OF BIDDERS(S) DATE: …….. ADDRESS …….. …….. ……..

SECTION 9

SBD 4

DECLARATION OF INTEREST

1. Any legal person, including persons employed by the state[1], or persons having a kinship with persons employed by the state, including a blood relationship, may make an offer or offers in terms of this invitation to bid (includes an advertised competitive bid, a limited bid, a proposal or written price quotation). In view of possible allegations of favouritism, should the resulting bid, or part thereof, be awarded to persons employed by the state, or to persons connected with or related to them, it is required that the bidder or his/her authorised representative declare his/her position in relation to the evaluating/adjudicating authority where-

   - the bidder is employed by the state; and/or

   - the legal person on whose behalf the bidding document is signed, has a relationship with persons/a person who are/is involved in the evaluation and or adjudication of the bid(s), or where it is known that such a relationship exists between the person or persons for or on whose behalf the declarant acts and persons who are involved with the evaluation and or adjudication of the bid.

2. **In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.**

2.1 Full Name of bidder or his or her representative: ……

2.1 Identity Number:……

2.2 Position occupied in the Company (director, trustee, shareholder[2], member):
……

2.3 Registration number of company, enterprise, close corporation, partnership agreement or trust:……..……

2.4 Tax Reference Number: ……

2.5 VAT Registration Number: ……

2.6.1 The names of all directors / trustees / shareholders / members, their individual identity numbers, tax reference numbers and, if applicable, employee / PERSAL numbers must be indicated in paragraph 3 below.

[1] "State" means –
(a) any national or provincial department, national or provincial public entity or constitutional institution within the meaning of the Public Finance Management Act, 1999 (Act No. 1 of 1999);
(b) any municipality or municipal entity;
(c) provincial legislature;
(d) national Assembly or the national Council of provinces; or
(e) Parliament.

[2]" Shareholder" means a person who owns shares in the company and is actively involved in the management of the enterprise or business and exercises control over the enterprise.

2.7 Are you or any person connected with the bidder presently employed by the state? **YES / NO**

2.7.1 If so, furnish the following particulars:

Name of person / director / trustee / shareholder/ member: ……..……

Name of state institution at which you or the person connected to the bidder is employed:

……
Position occupied in the state institution ……

Any other particulars:……

……

2.7.2 If you are presently employed by the state, did you obtain the appropriate authority to undertake remunerative work outside employment in the public sector? **YES / NO**

2.7.2.1 If yes, did you attach proof of such authority to the bid document? **YES / NO**

(Note: Failure to submit proof of such authority, where applicable, may result in the disqualification of the bid.

2.7.2.2 If no, furnish reasons for non-submission of such proof:

…….
…….
……

2.8 Did you or your spouse, or any of the company's directors / trustees / shareholders / members or their spouses conduct business with the state in the previous twelve months? **YES / NO**

2.8.1 If so, furnish particulars:
……..
……..
……...

2.9 Do you, or any person connected with the bidder, have any relationship (family, friend, other) with a person employed by the state and who may be involved with the evaluation and or adjudication of this bid? **YES / NO**

2.9.1 If so, furnish particulars.
……...
……..….
……

2.10 Are you, or any person connected with the bidder, aware of any relationship (family, friend, other) between any other bidder and any person employed by the state who may be involved with the evaluation and or adjudication of this bid? **YES/NO**

2.10.1 If so, furnish particulars**.**
……
……
……

2.11 Do you or any of the directors / trustees / shareholders / members of the company have any interest in any other related companies whether or not they are bidding for this contract? **YES/NO**

2.11.1 If so, furnish particulars:

…….
…….
…….

3 Full details of directors / trustees / members / shareholders

Full Name	**Identity Number**	**Personal Income Tax Reference Number**	**State Employee Number / Persal Number**

4 DECLARATION

I, THE UNDERSIGNED (NAME)……CERTIFY THAT THE INFORMATION FURNISHED IN PARAGRAPHS 2 and 3 ABOVE IS CORRECT. I ACCEPT THAT THE STATE MAY REJECT THE BID OR ACT AGAINST ME SHOULD THIS DECLARATION PROVE TO BE FALSE.

…….. ..……
Signature Date

……. ……
Position Name of bidder

SECTION 10

SBD 8

DECLARATION OF BIDDER'S PAST SUPPLY CHAIN MANAGEMENT PRACTICES

1 This Standard Bidding Document must form part of all bids invited.

2 It serves as a declaration to be used by institutions in ensuring that when goods and services are being procured, all reasonable steps are taken to combat the abuse of the supply chain management system.

3 The bid of any bidder may be disregarded if that bidder, or any of its directors have-
   a. abused the institution's supply chain management system;
   b. committed fraud or any other improper conduct in relation to such system; or
   c. failed to perform on any previous contract.

4 In order to give effect to the above, the following questionnaire must be completed and submitted with the bid.

Item	Question	Yes	No
4.1	Is the bidder or any of its directors listed on the National Treasury's Database of Restricted Suppliers as companies or persons prohibited from doing business with the public sector? (Companies or persons who are listed on this Database were informed in writing of this restriction by the Accounting Officer/Authority of the institution that imposed the restriction after the *audi alteram partem* rule was applied). **The Database of Restricted Suppliers now resides on the National Treasury's website (**www.treasury.gov.za**) and can be accessed by clicking on its link at the bottom of the home page.**	Yes ☐	No ☐
4.1.1	If so, furnish particulars:		
4.2	Is the bidder or any of its directors listed on the Register for Tender Defaulters in terms of section 29 of the Prevention and Combating of Corrupt Activities Act (No 12 of 2004)? **The Register for Tender Defaulters can be accessed on the National Treasury's website (www.treasury.gov.za) by clicking on its link at the bottom of the home page.**	Yes ☐	No ☐
4.2.1	If so, furnish particulars:		
4.3	Was the bidder or any of its directors convicted by a court of law (including a court outside of the Republic of South Africa) for fraud or corruption during the past five years?	Yes ☐	No ☐
4.3.1	If so, furnish particulars:		
4.4	Was any contract between the bidder and any organ of state terminated during the past five years on account of failure to perform on or comply with the contract?	Yes ☐	No ☐
4.4.1	If so, furnish particulars:		

SBD 8

CERTIFICATION

I, THE UNDERSIGNED (FULL NAME)……CERTIFY THAT THE INFORMATION FURNISHED ON THIS DECLARATION FORM IS TRUE AND CORRECT.

I ACCEPT THAT, IN ADDITION TO CANCELLATION OF A CONTRACT, ACTION MAY BE TAKEN AGAINST ME SHOULD THIS DECLARATION PROVE TO BE FALSE.

……...	**……..**
Signature	**Date**
……..	**……..**
Position	**Name of Bidder**

SECTION 11

SBD 9

CERTIFICATE OF INDEPENDENT BID DETERMINATION

1. This Standard Bidding Document (SBD) must form part of all bids[1] invited.
2. Section 4 (1) (b) (iii) of the Competition Act No. 89 of 1998, as amended, prohibits an agreement between, or concerted practice by, firms, or a decision by an association of firms, if it is between parties in a horizontal relationship and if it involves collusive bidding (or bid rigging).[2] Collusive bidding is a *pe se* prohibition meaning that it cannot be justified under any grounds.
3. Treasury Regulation 16A9 prescribes that accounting officers and accounting authorities must take all reasonable steps to prevent abuse of the supply chain management system and authorizes accounting officers and accounting authorities to:

    a. Disregard the bid of any bidder if that bidder or any of its directors have abused the institution's supply chain management system and or committed fraud or any other improper conduct in relation to such system.

    b. Cancels a contract awarded to a supplier of goods and services if the supplier committed any corrupt or fraudulent act during the bidding process or the execution of that contract.

4. This SBD serves as a certificate of declaration that would be used by institutions to ensure that, when bids are considered, reasonable steps are taken to prevent any form of bid-rigging.
5. In order to give effect to the above, the attached Certificate of Bid Determination (SBD 9) must be completed and submitted with the bid:

[1] Includes price quotations, advertised competitive bids, limited bids and proposals.

[2] Bid rigging (or collusive bidding) occurs when businesses, that would otherwise be expected to compete, secretly conspire to raise prices or lower the quality of goods and / or services for purchasers who wish to acquire goods and / or services through a bidding process. Bid rigging is, therefore, an agreement between competitors not to compete.

CERTIFICATE OF INDEPENDENT BID DETERMINATION

I, the undersigned, in submitting the accompanying bid:

_____

(Bid Number and Description)

in response to the invitation for the bid made by:

_____

(Name of Institution)

do hereby make the following statements that I certify to be true and complete in every respect:

I certify, on behalf of:_____that:

(Name of Bidder)

1. I have read and I understand the contents of this Certificate;

2. I understand that the accompanying bid will be disqualified if this Certificate is found not to be true and complete in every respect;
3. I am authorized by the bidder to sign this Certificate, and to submit the accompanying bid, on behalf of the bidder;
4. Each person whose signature appears on the accompanying bid has been authorized by the bidder to determine the terms of, and to sign the bid, on behalf of the bidder;
5. For the purposes of this Certificate and the accompanying bid, I understand that the word "competitor" shall include any individual or organization, other than the bidder, whether or not affiliated with the bidder, who:

    (a) has been requested to submit a bid in response to this bid invitation;
    (b) could potentially submit a bid in response to this bid invitation, based on their qualifications, abilities or experience; and
    (c) provides the same goods and services as the bidder and/or is in the same line of business as the bidder

6. 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 consortium[3] will not be construed as collusive bidding.
7. In particular, without limiting the generality of paragraphs 6 above, there has been no consultation, communication, agreement or arrangement with any competitor regarding:
    (a) prices;
    (b) geographical area where product or service will be rendered (market allocation)
    (c) methods, factors or formulas used to calculate prices;
    (d) the intention or decision to submit or not to submit, a bid;
    (e) the submission of a bid which does not meet the specifications and conditions of the bid; or
    (f) bidding with the intention not to win the bid.
8. In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications and conditions or delivery particulars of the products or services to which this bid invitation relates.
9. 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] 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.

10. 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.

……	……
Signature	Date
……	……
Position	Name of Bidder

SECTION 12

Confirmation

ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE SERVICES OFFERED BY YOU — YES / NO

Declaration

I/We have examined the information provided in your bid documents and offer to undertake the work prescribed in accordance with the requirements as set out in the bid document. The prices quoted in this bid are fixed and valid for the stipulated period. I/We confirm the availability of the proposed team members/ and or services. We confirm that this bid will remain binding upon us and may be accepted by you at any time before the expiry date.

Signature of bidder: .....

Date: .....

Are you duly authorized to commit the bidder: YES / NO

Capacity under which this bid is signed .....

Domicilium

NPA chooses the following as its domicilium citandi et executandi for all purposes of and in connection with the final contract:
NATIONAL PROSECUTING AUTHORITY, VGM BUILDING, WEAVIND PARK, 123 WEST LAKE AVENUE, SILVERTON, PRETORIA

The bidder must indicate its domicilium citandi et executandi for all purposes of and in connection with the final contract.

Any discrepancies between the information supplied here and the other parts of the bid may result in your bid being disqualified.

SECTION 13

ANNEXURE B: Bidder's Experience

Name of Bidder: …… **Bid Number. NPA 13-21/22**

[*Note to the Bidder: The bidder must complete the information set out below in full in response to the requirements stated in on Section 3,* ***paragraph 39.3*** *of this bid document. If the bidder requires more space than the provided below the bidder must prepare a document in same format setting out all the information referred to and return it with the proposal.]*

The bidder must provide the following information: (a) Details of the bidder's current and past projects of similar type, size and complexity to the required services set out for this bid.

Clients' Name, contact person and contact details	Project description	Project Cost	Project period (Start and End Dates)	Description of service performed and extent of Bidder's responsibilities