

PIC011/2020: REQUEST FOR PROPOSAL FOR THE APPOINTMENT OF A SUITABLY QUALIFIED BIDDER FOR THE PROVISION, IMPLEMENTATION, SUPPORT AND MAINTENANCE OF A VULNERABILITY MANAGEMENT SOLUTION FOR A PERIOD OF THREE (3) YEARS WITH POSSIBILITY OF EXTENSION FOR A FURTHER TWO (2) YEARS

The Public Investment Corporation (PIC) is a registered Financial Service Provider (FSP) and a public entity, wholly owned by the South African Government. PIC invests funds on behalf of public sector entities. Among the PIC's clients are the Government Employees Fund ("GEPF"), Unemployment Insurance Fund ("UIF") and Compensation Fund ("CP"):

The PIC therefore seeks proposals from a suitably qualified bidder with a proven track record of successfully designing, implementing and providing comprehensive support of a Vulnerability Management Solution.

The successful bidder will be required to provide maintenance and support of the provisioned solution for a period of three (3) years with a possibility of extending for two (2) more years. The main objective for considering the Vulnerability Management Solution is to provide a secure environment IT environment in order to support business modernisation strategy.

The key benefits that are expected by the PIC from the proposed Vulnerability Management include but are not limited to the following:

- Pinpoint all Information Security risks on the PIC IT infrastructure;
- Provide capability to proactively identify security vulnerabilities;
- Define the level of risk that exists on the PIC IT network, systems and advice on remediation for identified vulnerabilities;
- Provide asset discovery capabilities and create an inventory of all PIC networked devices.

Bid documentation will be available on the PIC website: www.pic.gov.za. The Documents will be published on tenders/corporate/Advertised/PIC011/2020 from 3 August 2020.

Briefing session slides will be available on the PIC website from 10 August 2020.

Closing date for the bid submission: 4 September 2020, Closing time: 11:00 AM
Proposals must be submitted electronically to tenders@pic.gov.za. Reference number: PIC011/2020 must be indicated in all correspondence.

Enquiries: tenders@pic.gov.za

**BID NO (PIC011/2020): REQUEST FOR PROPOSAL
FOR THE APPOINTMENT OF A SUITABLY QUALIFIED BIDDER
FOR THE PROVISION, IMPLEMENTATION, SUPPORT AND
MAINTENANCE OF A VULNERABILITY MANAGEMENT
SOLUTION FOR A PERIOD OF THREE (3) YEARS WITH
POSSIBILITY OF EXTENSION FOR A FURTHER TWO (2) YEARS**

Bid Number : PIC 011/2020
Closing Date : 4 September 2020
Closing Time : 11:00 AM
Place of Submission : Electronic submission: tenders@pic.gov.za

No briefing session: Slides will be available on PIC website from 10 August 2020

Validity period of bid: 180 days

TABLE OF CONTENTS

1	DEFINITIONS AND ABBREVIATIONS	4
2	INTRODUCTION.....	6
3	BACKGROUND.....	7
3.10.1.	In-Scope	9
4	PIC VULNERABILITY MANAGEMENT BUSINESS REQUIREMENTS	10
4.1	Business Requirements.....	10
4.2	Minimum Requirements.....	Error! Bookmark not defined.
5	PROJECT MANAGEMENT SERVICES.....	18
6	CLIENT REFERENCES	20
7	PROJECT TEAM EXPERIENCE.....	20
8	SERVICE MANAGEMENT.....	21
9	EVALUATION CRITERIA AND METHODOLOGY.....	22
10	ADMINISTRATIVE REQUIREMENTS.....	23
11	TECHNICAL / FUNCTIONAL SCORING CRITERIA.....	24

12	PRICING PROPOSAL.....	29
13	PROPOSED RESPONSES FORMAT	30
14	CONDITIONS	34
17	PART A SBD 1.....	38
18	DECLARATION OF INTEREST	44
19	COMPANY INFORMATION.....	49
20	DECLARATION	52
	PUBLIC INVESTMENT CORPORATION SOC LIMITED	54

1 DEFINITIONS AND ABBREVIATIONS

- 1.1 **B-BBEE** means black broad-based economic empowerment;
- 1.3 **B-BBEE** status level of contributor means the B-BBEE status received by a measured entity based on its overall performance using the relevant scorecard contained in the Codes of good practice on Black Economic Empowerment, issues in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act;
- 1.4 **Bid** means a written offer in a prescribed or stipulated form in response to an invitation by PIC for the provision of goods and services, through price quotations, advertised competitive tendering processes or proposals;
- 1.5 **BBEE Act** means the Broad Based Black Economic Empowerment Act, 2003 (Act No. 53 of 2003);
- 1.6 **Cisco** means Networking Infrastructure, PIC internet Security Gateway
- 1.6 **CEH** means Certified Ethical Hacker
- 1.7 **Consortium or joint venture** means an association of persons for the purpose of combining their expertise, property, capital, skill and knowledge in an activity for the execution of a contract;
- 1.8 **Contract** means the agreement that results from the written acceptance of a bid by the PIC and successful negotiation and signature of same by both parties delegated authorities;
- 1.9 **CISSP** means Certified Information Systems Security Professional
- 1.10 **DMZ** means Demilitarized Zone (sometimes referred to as a perimeter network)
- 1.11 **Functionality** means the measurement according to predetermined norms, as set out in the bid documents, of a service or commodity that is designed to be

practical and useful, working or operating, taking into account among other factors, the quality, reliability, viability and durability of a service and the technical capacity and ability of a bidder;

- 1.12 **Information Security means** the state of being protected against the unauthorized use of information, especially electronic data
- 1.13 **IT Systems** means Citrix, UNIX, Network infrastructure, Databases and all other Microsoft systems and applications.
- 1.14 **Management** means an activity inclusive of control and performed on a daily basis, by any person who is a principal executive officer of the company, by whatever name that person may be designated, and whether or not that person is a director;
- 1.15 **Microsoft SCCM** means Microsoft Systems Centre Configuration Manager
- 1.16 **OSCP** means Offensive Security Certified Professional
- 1.17 **Ownership** means the percentage ownership and control, exercised by individuals within an enterprise;
- 1.18 **PPPFA** means the Preferential Procurement Policy Framework Act, 2000 (Act No 5 of 2000);
- 1.19 **POPIA** means the Protection of Personal Information Act, 2013 (Act No 4 of 2013)
- 1.20 **SANAS** means the South African National Accreditation System;
- 1.21 **Validity Period** means the time period for which price quotation for the provision of goods and services shall remain valid, in this case, being a period of 120 (one hundred and twenty) days;
- 1.22 **Vulnerability Management means** A set of technologies and techniques that are created to prevent sensitive information from leaving a company

2 INTRODUCTION

The Public Investment Corporation (PIC) is an asset management company wholly owned by the government of the Republic of South Africa duly represented by the Minister of Finance. The PIC manages investments on behalf of public sector funds which include Government Employees Pension Fund (GEPF), Unemployment Insurance Fund (UIF) and Compensation Fund. Established in 1911, the PIC ranks amongst the best and most successful asset management firms in the world and is by far the biggest in Africa. The PIC runs one of the most diversified portfolios, which is made-up of multiple asset classes. These asset classes include listed equities, real estate, capital market, private equity and impact investing. Through listed investments, the PIC controls over 10% of the Johannesburg Stock Exchange and has direct and indirect exposure to almost all sectors of the South African economy. The corporation has a mandate to invest in the rest of the African continent and beyond. Over and above generating financial returns for clients, through its impact-investing programme, the PIC seeks to generate social returns by investing in projects that ensure inclusive growth. The PIC supports the United Nations' Sustainable Development Goals and considers environmental, social and governance issues in all its investments.

The PIC manages assets exceeding R2 trillion; and as the leader in the Asset Management industry, it thrives to meet and exceed its clients' expectations.

3 BACKGROUND

3.1. The PIC is in a process of modernizing its processes in an effort to achieve its strategic objectives such as, but not limited to the following:

3.1.1 Fulfilling and exceeding its client expectations by investing in sustainable growth, inclusivity, and transformation;

3.1.2 Becoming a catalyst for continental integration and a global investor;
and

3.1.3 Growing our client base and investment products offering through innovative thinking.

3.2. To successfully achieve this, the PIC requires the use of Information Technology solutions necessary to enable seamless Investment Management processes and related digital business changes;

3.3. As part of the approved business modernization strategy, the PIC seeks to ensure that its information technology landscape includes capabilities to secure its private information through the implementation of tools that provide capabilities to identify, classify, prioritize, remediate and mitigate vulnerabilities on its information technology infrastructure;

3.4. As a result, the PIC's Information Security division has a responsibility to establish business processes that will assist in the protection, securing and monitoring of the organisation technology infrastructure in order to enable the achievement of strategic and operational objectives of the organisation;

- 3.5. The PIC therefore seeks to solicit proposals from and appoint suitably qualified bidder with a proven track record of successfully designing, implementing and providing comprehensive support of a Vulnerability Management Solution;
- 3.6. The successful bidder will be required to provide maintenance and support of the provisioned solution for a period of three (3) years with a possibility of extending for two (2) more years;
- 3.7. The main objective for considering the Vulnerability Management Solution is to provide a secure environment IT environment in order to support business modernisation strategy;
- 3.8. The key benefits that are expected by the PIC from the proposed Vulnerability Management include but are not limited to the following:
 - 3.8.1. Pinpoint all Information Security risks on the PIC IT infrastructure;
 - 3.8.2. Provide capability to proactively identify security vulnerabilities;
 - 3.8.3. Define the level of risk that exists on the PIC IT network, systems and advice on remediation for identified vulnerabilities;
 - 3.8.4. Provide asset discovery capabilities and create an inventory of all PIC networked devices.
- 3.9. The scope of work defines the work what is to be done including specific tasks and detailed information about the expected deliverables;
- 3.10. The vulnerability management project will cover the entire PIC IT network comprising of external, internal, and systems including cloud based systems and will include the following but not limited to the following in Scope areas:

3.10.1. In-Scope

3.10.1.1. Asset Discovery

3.10.1.1.1. The ability to have a current, updated enterprise asset inventory is critical to the success of the PIC vulnerability management program.

The solution should be able to discover systems using IP address ranges(agentless);

3.10.1.1.2. The PIC together with the service provider will complete an inventory and blueprint of the PIC networked technology assets. This will be completed through a network discovery process, which is expected to produce a comprehensive inventory detailing the organisations services, workstations, network devices, laptop etc.

3.10.1.2. Vulnerability Assessment Scans

3.10.1.2.1. The vulnerability management services and solution is expected to assist the PIC in proactively close any gaps and maintain a strong security environment for PIC network and systems. Data breaches are often the result of vulnerabilities, so identifying and eliminating these security gaps, removes that attack vector.

3.10.1.3. Reporting

3.10.1.3.1. Vulnerability Management report provides a high-level overview of an organization's vulnerability management program. These reports assist the information security division in identifying and tracking security issues in all phases of the cyber exposure lifecycle,

translating raw security data into a common language for communicating risk back to the organization;

3.10.1.3.2. The PIC vulnerability management solution must provide capabilities to produce detailed vulnerability reports that include date of vulnerability discovery, severity score of the vulnerability based on common vulnerability and exposures, detailed description of vulnerabilities etc. The solution must provide an ability to draw selective reports and identify repeat findings.

4 PIC VULNERABILITY MANAGEMENT BUSINESS REQUIREMENTS

In addition, the following requirements are to be met as part of the Vulnerability Management Solution implementation at the PIC:

4.1 Business Requirements

#	Description	Comply	Not Comply	Comments	Ref of RFP Response
	Vulnerability Scanning				
4.1.1	The solution must have automated asset discovery capabilities;				

4.1.2	<p>The solution must provide an ability to scan the network and systems for vulnerabilities using:</p> <p>Authenticated Scan: authenticated scan is a vulnerability scan that is performed by an authenticated user– a user with login credentials with capabilities to run deep scanning; and</p> <p>Non-authenticated Scan: non-authenticated scan performs a vulnerability scan by not using usernames or passwords during the scanning.</p>				
4.1.3	<p>The solution must perform automated or ethical exploits to verify the discovered vulnerabilities, while ensuring an uninterrupted network and systems operation and/or availability.</p>				
4.1.4	<p>Vulnerability Scanning on all network and systems including Cloud based systems.</p>				
4.1.5	<p>The solution must provide capabilities to perform web application vulnerability</p>				

	scanning to identify all related vulnerabilities such as OWASP vulnerabilities and other vulnerabilities.				
4.1.6	Provide vulnerability alerting capabilities.				
4.1.7	Provide capabilities to identify and eliminating false positives and false negatives.				
4.1.8	The bidder must be able to provide assurance that the solution detects the most minimum rate of false positives and false negatives, with a capability to fine tune false positive and false negative occurrences.				
4.1.9	Provide a solution that has capabilities to monitor vulnerabilities introduced by applications installed on PIC IT infrastructure components such as laptop computers etc.				
4.1.10	In addition to being able automatically start vulnerability scans on discovery of new devices on the PIC IT infrastructure, the solution must provide capabilities to				

	schedule scans to avoid impacting network performance.				
4.1.11	<p>The solution must be able to provide a holistic view of the environment where the PIC information security team is able to drill down at any stage to explore the following but not limited to:</p> <ul style="list-style-type: none"> • Assets; • Applications and Systems; • Vulnerabilities; • Operating systems. 				
4.1.12	Vulnerability assessment scans should be able to target individual assets, asset groups, or even entire networks.				
4.1.13	The solution must be able to automatically pause scheduled scans if unable to complete within the predefined durations in a secured manner.				
4.1.14	The solution must have the ability to associate a severity value to each vulnerability discovered based on the				

	common vulnerability scoring system score CVSS and CVE number for each of the discovered vulnerabilities.				
4.1.15	The solution must have capabilities to automatically prioritize vulnerabilities based on pre-set rules and business risk.				
4.1.16	Customized prioritization using business context capability.				
4.1.17	Identify network misconfigurations on the PIC network and all systems including cloud based systems.				
4.1.18	The vulnerability management solution should also be setup to allow PIC Personnel to run adhoc vulnerability scans on the environment, to scan new devices and systems.				
	The proposed solution should be able to on-board systems using IP ranges.				
4.1.19	The solution must provide a centrally managed capability to automatically scan and identify vulnerabilities from all sources in the PIC network and systems.				

4.1.20	The solution must be able to determine protocol, service or application version running on each open port.				
4.1.21	The solution must cover all platforms.				
4.1.22	Ability to integrate with any vulnerability scanning tools and existing security tools to aggregate, normalize, prioritize, correlate and improve all of the vulnerability data.				
4.1.23	Automated vulnerability remediation response workflows.				
4.1.24	Provide capability to integrate with various incident logging solution.				
	Reporting				
4.1.25	Reporting function of the solution must have the following reports but not limited to: <ul style="list-style-type: none"> • Automated and comprehensive devices discovery Report; • Identification of actors involved; • Scheduled Comprehensive vulnerability scanning reports; 				

	<ul style="list-style-type: none"> • Vulnerability scanning Report that indicate REPEAT findings; • Dashboards Reports; • Indicators of Compromise; • Major security changes needed; etc. 				
4.1.26	Provide capability to automatically assign vulnerabilities to SME's within the PIC for resolution.				
4.1.27	Ability to tailor dashboard presentation to client needs.				
4.1.28	Intelligent reporting capabilities, including Executive management reporting, High level and detailed analysis of top assets and networks affected by discovered vulnerabilities				
4.1.29	Ability to use reports and customizable data views to organize threats and vulnerabilities by severity to assist in better prioritization of mitigating controls				
4.1.30	KPI monitoring of vulnerability management program capability.				

4.1.31	Provide capabilities to automate capturing vulnerability remediation's as part of the workflow capabilities.				
Technical Requirements					
4.1.32	The solution is expected to operate on all platforms				
4.1.33	The solution must be user-friendly with a portal for PIC IT to conduct the following but not limited to: <ul style="list-style-type: none"> • User Management; • Monitoring of overall health of all components. 				
4.1.34	The solution should be able to integrate with PIC cloud based systems.				
4.1.35	The solution must be able to integrate with all and future PIC solutions including the SIEM solution.				
Auditing Requirements					
4.1.36	Keep an audit trail of all vulnerabilities and applied remediation steps				

4.1.37	The bidder is required to conduct a POC for the PIC to demonstrate the functionality of their proposed solution.				
--------	--	--	--	--	--

4.2 Minimum Requirements

The bidder must comply to the following **minimum requirements** in order to respond to this RFP. Bidders who are **NOT compliant** will be **disqualified**.

4.2.1 The Bidder must have a minimum of ten (10) years in operation and implementing vulnerability management services similar to those required by the PIC;

Indicate paragraph no and page no where this information can be referenced in proposal.

4.2.2 The technical lead must have a minimum of five (5) years' experience in the Information Security Field and possess the relevant Information Security

Qualifications:

Indicate paragraph no and page no where this information can be referenced in proposal.

5 PROJECT MANAGEMENT SERVICES

The PIC recognizes the extent of the scope of work that the vendor will be engaging in to implement the technical architectural design and implementation of the desired solution.

The PIC further recognizes the importance of employing the correct delivery model from the onset.

This will ensure that there is proper planning, phase identification and prioritization, improved coordination; reduced risk and the eventual execution is seamless.

The Bidder must provide Project Management Services for the full implementation of the solution. The Bidder must also provide detailed description of their Project Management process/ methodology in sufficient detail to convey to the PIC that it is capable to implement its proposed service on time and on budget. The methodology must indicate clear stage gates which require approval and signoff, triggering payment on completion of key milestones.

The PIC expects the service provider to provide project documentation, from Project initiation document, project plan, requirements analysis, system architecture, solution documentation and design documents, test plans, training and technical documentation. The bidder shall clearly specify the proposed approach, methodology and plan for the implementation of the Vulnerability Management Solution.

These include but are not limited to the following:

- Delivery, configuration, deployment and operation of the Vulnerability Management Solution.
- Provide an implementation plan covering service, deliverables and skills.
- A centralized operational reporting and administration web interfaces for administration, configuration, reporting and workflow.
- Comply with internal policies and audit controls.
- Provide Change Management service to the PIC.
- Skills transfer and training of PIC personnel.

6 CLIENT REFERENCES

Bidder must provide a list of at least 4(four) contactable clients references of companies where similar work has been successfully delivered within the last 5 (five) years. Bidder must include reference letters from clients;

The PIC may use the references provided as a basis for which client sites will be visited. For shortlisted Bidder, the PIC may require assistance to arrange site visits. References details must include the following:

- 6.1. The name of the entity, contact person, designation of contact, contact number, and date; and
- 6.2. Reference letter from client confirming the Vulnerability Management Solution implementation.

7 PROJECT TEAM EXPERIENCE

- 7.1. Bidder's must provide a summary of the company's staff compliment and CV details/experience of the team to be assigned to this project.
 - 7.1.1. Experience of the core project team to be involved in the implementation of the project and years of experience must have a minimum of 10 years combined (Excluding the IT technical lead);
 - 7.1.2. IT Technical Lead must have a minimum of 10 years' experience implementing Vulnerability Management Solutions;
 - 7.1.3. CV's and valid security certifications for all the team members assigned to the project must be provided;
 - 7.1.4. The IT technical lead response must include a table with Client, Project Implemented, Project Start and End Dates, Client Contact Details.

NB: The bidder must have additional resources with similar experience as technical lead to cover when one resource is not available in order to reduce key mad dependency risk;

7.2. The technical resources assigned to this project are expected to have a combination of experience and the following certifications:

7.2.1. Certification in the Vulnerability Management Solution that will be implemented;

Certification	Comply	Not Comply	Comments	Ref in Response
Certified Ethical Hacker(CEH)				
Offensive Security Certified Professional (OSCP).				
Additional Certifications	Comply	Not Comply	Comments	Ref in Response
SANS certifications such as the Global Information Assurance Certification Global Information Assurance Certification				

Valid certified copies of the resources' certifications must be included for verification.

8 SERVICE MANAGEMENT

The Bidder must provide Service Level Agreements for Support and Maintenance for a period of 3 years stipulating and inclusive of the following:

- **Premium support inclusive but not limited to the following:**
 - **99.9% Availability of the Solution**

- **Service Levels:** Service Priority Levels and associated Turnaround times as follows:

Priority/ Severity	Response Turn Around Time	Resolution Turn Around Time
1	Within 30 Minutes	Within 2 business hours
2	Within 30 Minutes	Within 4 business hours
3	Within 1 hour	Within 8 business hours

- Relationship Management Activities
- Services credit methodology in case of a Service Level Breach; and
- Sample service level reporting

9 EVALUATION CRITERIA AND METHODOLOGY

The evaluation criteria will be based on the following requirements:

- **Phase 1:** Compliance to administrative requirements
- **Phase 2:** Minimum Requirements
- **Phase 3:** Technical Functional Requirements (100 points).

Bidder, who score below 70 points, will not go through to the next level of evaluations. **Presentations** and site visits may part of the technical evaluation. (Bidder who score 70 or more points out of 100 points allocated at technical evaluation will be subjected to site visits and further evaluated on price and B-BBEE upon confirmation of infrastructure during site visits).

Price and BEE Evaluations (80/20 points).

- **Phase 4: Pricing Proposal**

Bidder(s) who fail to comply phase 1 and 2 requirements will not proceed to the next phases

10 ADMINISTRATIVE REQUIREMENTS

The Bidder will proceed to the next stage when they comply with the requirements stated herein below.

The bidder will proceed to the next stage when they comply with the following requirements:

Submission of:

- A valid and original Tax Clearance Certificate/Valid Tax Pin Number.
- *BBBEE status level certificate –Accredited by SANAS (If no BEE certificate is submitted/or BEE certificate submitted is not valid, no points will be allocated for BEE).
- *EME's and QSE's –sworn Affidavit
- *Signed and completed declaration of interest document
- *Signed and completed SBD 1 – Invitation to Bid document
- *Signed and completed Company Information document
- *Latest audited Financial statements within the last two years
- *Completed and signed Company Information document and submission of all the required documentation as stipulated in the company profile document
- Acceptance of the conditions as stipulated in the bid document
- Submission of all attached as per the bid evaluation criteria, the bid document and a separate pricing proposal

- The CSD (Central Supplier Database) is a single source of all supplier information for all spheres of government and all suppliers engaging with the PIC should be registered on the CSD. Kindly enclose your CSD registration number
- Bid Documents (1 x Technical and Administrative proposal and 1 x Fee proposal to be submitted as separate documents) to be submitted **electronically** to tenders@pic.gov.za quoted reference number PIC011/2020
- All the documents must be in PDF format and be clearly indexed

11 TECHNICAL / FUNCTIONAL SCORING CRITERIA

With regards to technicality / functionality, the following criteria shall be applicable, and the maximum points of each criterion are indicated in the table below:

Technical / Functional Criteria	Weightings
<p>12.1 Project Management</p> <p>Elements: Submission by bidder must include an adequate and clear plan on project management (including assessment and implementation) of Vulnerability Management Solution at the PIC.</p> <p>The proposed project management plan must include details on the following:</p> <ul style="list-style-type: none"> • Project Methodology (including Project Management & Governance, Change Management and Risk Management) • PIC services offering Readiness Assessment (with recommendations) • PIC services Roadmap • Implementation Plan (including migration) • Post Implementation - stabilisation, service delivery and support (including managed services life cycle) 	<p>5</p>

Technical / Functional Criteria	Weightings																																			
<p data-bbox="193 501 1219 539">12.2 Technical Lead – Years of experience in implementing Vulnerability Management Solutions</p> <p data-bbox="193 568 1219 607">Management Solutions</p> <p data-bbox="193 703 1219 875">The Technical Lead must have a minimum of ten (10) years (e.g. from 2010 to current) technical lead experience on Vulnerability Management Solutions as per scoring matrix below</p> <p data-bbox="193 972 1219 1346">Please provide copies and information security certification of the C.V. of the Technical Lead and the project team that will be responsible for the implementation, implementation and support of the PIC Vulnerability Management Solution. In addition, the table below must be completed and included in the bid proposal section with the C.V. Failure to include the table will result in non-consideration of the C.V</p> <table border="1" data-bbox="209 1375 1203 1854"> <thead> <tr> <th data-bbox="209 1375 320 1581">Client</th> <th data-bbox="320 1375 533 1581">Project Implemented</th> <th data-bbox="533 1375 667 1581">Budget</th> <th data-bbox="667 1375 778 1581">Start Date</th> <th data-bbox="778 1375 890 1581">End Date</th> <th data-bbox="890 1375 1066 1581">Relevance to Service Offerings</th> <th data-bbox="1066 1375 1203 1581">Client Contact Details</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> </tr> </tbody> </table>	Client	Project Implemented	Budget	Start Date	End Date	Relevance to Service Offerings	Client Contact Details																													<p data-bbox="1219 501 1402 539">10</p>
Client	Project Implemented	Budget	Start Date	End Date	Relevance to Service Offerings	Client Contact Details																														

Technical / Functional Criteria	Weightings
<p>12.3 Company Experience (References)</p> <p>Please provide A MINIMUM of four (4) recent) attestation letters from the respective customers on the letterheads CONFIRMING IMPLEMENTATION of a Vulnerability Management Scope Services.</p> <p>The letters MUST INCLUDE the company name, the services offered, contact person, contact numbers.</p> <p>Please note: The PIC will not accept a list of references and/or references listed on a table. The reference letters must be in the form of individual letters from the respective customers.</p>	<p>10</p>

Technical / Functional Criteria	Weightings																					
<p>12.4 Compliance to the PIC Vulnerability Management Solution scope</p> <p>Bidder must illustrate current capability and capacity to meet PIC Vulnerability Management Solution Business requirements plus, Bidder must illustrate their future growth plans:</p> <table border="1" data-bbox="209 837 1219 1447"> <thead> <tr> <th data-bbox="209 837 703 972">Vulnerability Management Solution Scope Item</th> <th data-bbox="703 837 839 972">Weight</th> <th data-bbox="839 837 1219 972">Section in Proposal</th> </tr> </thead> <tbody> <tr> <td data-bbox="209 972 703 1106">Vulnerability Management Solution Scope</td> <td data-bbox="703 972 839 1106">10</td> <td data-bbox="839 972 1219 1106"></td> </tr> <tr> <td data-bbox="209 1106 703 1171">Business Requirements</td> <td data-bbox="703 1106 839 1171">20</td> <td data-bbox="839 1106 1219 1171"></td> </tr> <tr> <td data-bbox="209 1171 703 1236">Technical Requirements</td> <td data-bbox="703 1171 839 1236">15</td> <td data-bbox="839 1171 1219 1236"></td> </tr> <tr> <td data-bbox="209 1236 703 1301">Audit Requirements</td> <td data-bbox="703 1236 839 1301">5</td> <td data-bbox="839 1236 1219 1301"></td> </tr> <tr> <td data-bbox="209 1301 703 1366">Minimum Requirements</td> <td data-bbox="703 1301 839 1366">15</td> <td data-bbox="839 1301 1219 1366"></td> </tr> <tr> <td data-bbox="209 1366 703 1447">Value Adds</td> <td data-bbox="703 1366 839 1447">5</td> <td data-bbox="839 1366 1219 1447"></td> </tr> </tbody> </table> <p>The Bidder must provide the above table as an attachment to the RFP response to the PIC Datacentres & Converged Infrastructure requirements. *All value adds must be clearly articulated and referenced as per the table above.</p>	Vulnerability Management Solution Scope Item	Weight	Section in Proposal	Vulnerability Management Solution Scope	10		Business Requirements	20		Technical Requirements	15		Audit Requirements	5		Minimum Requirements	15		Value Adds	5		<p>70</p>
Vulnerability Management Solution Scope Item	Weight	Section in Proposal																				
Vulnerability Management Solution Scope	10																					
Business Requirements	20																					
Technical Requirements	15																					
Audit Requirements	5																					
Minimum Requirements	15																					
Value Adds	5																					

Technical / Functional Criteria	Weightings
<p>12.5 Service Level Agreement</p> <p>Bidder must:</p> <p>Propose SLAs inclusive of the following as per section 9:</p> <ul style="list-style-type: none"> - Premium support inclusive but not limited to the following: <ul style="list-style-type: none"> ○ 99.9% Availability of the Solution ○ Service Priority Levels and associated Turnaround times as per section 9. - Relationship Management Activities - Services credit methodology in case of a Service Level Breach; and - Sample service level reporting 	<p>5</p>

12 PRICING PROPOSAL

Bidders are required to submit a proposal for all services outlined in the Scope of work. The costs for the Bidder's proposal should be submitted in a separate document in line with the Scope of Work identified. It is the responsibility of the Bidder to ensure the accuracy of the pricing provided as part of the response.

Costs should include the complete, fixed costs (if not fixed please indicate and provide details) for the services requested, including but not limited to the following:

All costs should be completely reflected on the pricing proposal.

When completing the Pricing Bidder must take note of the following:

- All pricing (including services, resources, hourly rates charged etc.) to be quoted in South African Rand including VAT. Pricing should be in alignment with the National Treasury.
- Bidders to incorporate pricing assumptions which will include:
 - Forex;
 - Licensing fees; and
 - Price fluctuations.
- Pricing assumptions must cater for growth of PIC staff complement.
- Pricing must show clearly the once off implementation cost and ongoing maintenance cost.

- Disbursements will be discussed and agreed during contract negotiations in line with the PFMA and/or National Treasury Regulations.

Pricing should follow this format considering the outlined deliverables specified in the tender document.

PIC Vulnerability Management Solution	Once-Off Costs (e.g. Transitioning and Implementation services)	Monthly Maintenance & Support	Monthly Fee	Annual Fees(e.g. Licensing Fees)	Sub-Totals	Explain Basis for Total Monthly Fee / Comments
Vulnerability Management						
Backup & Recovery						
Other (add a row for each category)						
TOTALS:						N/A

For the purpose of ease in evaluating the **Functionality of bids**, Bidder are required to present their bid documentation under the following headings:

Reference	Title	Guideline
Section 1	Cover letter	Brief company background, services and expertise, contact name and details of delegate authorized to make representations for the organization.
Section 2	Understanding of the PIC Requirements	Outline your understanding of the PIC Request for Proposal
Section 4	Scope of Work	Respond and cover all items presented for Vulnerability Management Solution.
Section 5	Project Management Services	Respond and cover on how the project will be approached and planned.
Section 6	Bidder Experience	Provide summary of the company's experience in the nature of the services required and staff compliment and CV details/experience of the team to be assigned to this project.
Section 7	Client References	Provide a summary of client references
Section 9	Service Management	Should cover the proposed SLA, support and maintenance plan for a period of 5 years
Section 13	Pricing Proposal	Cover all costs in detail as per pricing proposal details

Phase 3: PRICE AND BEE EVALUATION

All Bidder to submit their pricing as per schedule below-

- (a) Annual increases must not exceed CPI related to the specific year;
- (b) A maximum of 80 points is allocated for price on the following basis:

Where

P = Points scored for price of bid under consideration

Pt. = Rand value of bid under consideration

Pmin = Rand value of lowest acceptable bid

Points will also be awarded based to a bidder for attaining their B-BBEE status level of contribution in accordance with the table below:

B-BBEE Status Level of Contributor	Number of points /20
1	20
2	18
3	14
4	12
5	8
6	6
7	4
8	2

Non-compliant Contributor	0
---------------------------	---

List of Shareholders

Name	ID No	SA Citizen	Race	Gender	Shareholding %

- 15.7 Points scored will be rounded off to the nearest two decimal places.
- 15.8 The Bidder who scored the highest point will be awarded the bid.
- 15.9 In the event where two or more Bidder scored equal points, the successful bidder must be the one scoring the highest preference points for BBBEE.
- 15.10 However, when functionality is part of the evaluation process and two or more Bidder have scored equal points including equal preference points for BBBEE, the successful bidder must be the one scoring the highest for functionality.

15.11 Should two or more Bidder be equal in all respects; the award shall be decided by the drawing of lots.

14 CONDITIONS

16.1 Joint Ventures / Consortiums

16.1.1 The following information and documentation must be submitted:

16.1.1.1 All information stipulated in paragraph 10 under minimum and administrative requirements must be submitted by all parties involved in the Joint Ventures/Consortiums, including ownership and executive management information.

16.1.1.2 A percentage breakdown of the work allocation between the parties must be clearly indicated.

16.1.1.3 A formal signed agreement indicating the leading company as well as the other company roles and responsibilities must be submitted.

16.1.1.4 A skills transfer plan between the parties must be submitted.

16.2 Non-Commitment

16.2.1 The PIC reserves the right to withdraw or amend these terms of reference by notice in writing to all parties who have received the terms of reference prior to the closing date.

16.2.2 The cost of preparing of bids will not be reimbursed.

16.3 Reasons for rejection

16.3.1 The PIC reserves the right to reject bids that are not according to specification/Terms of Reference. Bidder must clearly indicate compliance or non-compliance with specification/Terms of Reference.

16.3.2 Bidder shall not contact the PIC on any matter pertaining to their bid from the time the bids are closed to the time the bid has been adjudicated. Any effort by a bidder to influence the bid evaluation, bid comparisons or bid award decisions in any matter, may result in rejection of the bid concerned.

16.3.3 The PIC shall reject a submission if the Bidder has committed a proven corrupt or fraudulent act in competing for a particular contract.

16.3.4 The PIC may disregard any submission if that Bidder, or any of its directors -

16.3.3.1 have abused the Supply Chain Management (SCM) system of any Government Department/ institution;

16.3.3.2 have committed proven fraud or any other improper conduct in relation to such system;

16.3.3.3 have failed to perform on any previous contract and the proof thereof exists; and/or

16.3.3.4 Is restricted from doing business with the public sector if such a bidder obtained preferences fraudulently or if such bidder failed to perform on a contract based on the specific goals.

16.4 Cancellation of Bid

16.4.1 The PIC may prior to the award of a bid, cancel a bid for the following reasons -

16.4.1.1 due to changed circumstances, there is no longer a need for the goods or services requested;

16.4.1.2 funds are no longer available to cover the total envisaged expenditure;

16.4.1.3 no acceptable bids are received

16.4.1.4 unsuccessful contract negotiations

16.4.2 The PIC may after award of the tender but before conclusion of a contract, cancel a bid for the following reasons-

16.4.2.1 due to change of circumstances, there is no longer a need for the goods or services requested;

16.4.2.2 funds are no longer available to cover the total envisaged expenditure.

16.5 Clarifications

Any clarification required by a bidder regarding the meaning or interpretation of the document, or any other aspect concerning the submission, is to be requested in writing e-mail to tenders@pic.gov.za .

Clarifications questions must be provided by no later the 25 August 2020 and responses will be provided by the 28 August 2020.

16.6 Receipt of Bids

Bids to be submitted electronically to tenders@pic.gov.za

16.7 Late Bids

No late bids will be accepted.

16.8 Presentations

The PIC may require presentations and/or site visits at a stipulated date and time from short-listed Bidder as part of the bid process.

16.9 Service Level Agreement (SLA)

16.9.1 The SLA will set out the administration processes, service levels and timelines.

16.9.2 The award of a tender shall always be subject too successful negotiation and conclusion of an SLA / contract. There will be no binding agreement between the parties if a contract has not been concluded.

16.10 Contracting

Bidder are advised that a valid contract will only come into existence between the PIC and the successful bidder after conclusion of successful negotiations and signature of the Contract by both parties' respective delegated authorities.

INVITATION TO BID

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE PUBLIC INVESTMENT CORPORATION				
BID NUMBER:	PIC011/2020	CLOSING DATE:	4 September 2020	CLOSING TIME: 11:00 AM
DESCRIPTION	APPOINTMENT OF A SUITABLY QUALIFIED BIDDER FOR THE IMPLEMENTATION OF A VULNERABILITY MANAGEMENT SOLUTION FOR A PERIOD OF THREE YEARS			
BID RESPONSE DOCUMENTS MAY BE DEPOSITED IN THE BID BOX SITUATED AT (STREET ADDRESS)				
tenders@pic.gov.za				
BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO			TECHNICAL ENQUIRIES MAY BE DIRECTED TO:	
CONTACT PERSON			CONTACT PERSON	
TELEPHONE NUMBER			TELEPHONE NUMBER	
FACSIMILE NUMBER			FACSIMILE NUMBER	
E-MAIL ADDRESS			E-MAIL ADDRESS	
SUPPLIER INFORMATION				
NAME OF BIDDER				
POSTAL ADDRESS				
STREET ADDRESS				
TELEPHONE NUMBER	CODE		NUMBER	
CELLPHONE NUMBER				
FACSIMILE NUMBER	CODE		NUMBER	
E-MAIL ADDRESS				

VAT REGISTRATION NUMBER				
SUPPLIER COMPLIANCE STATUS	TAX COMPLIANCE SYSTEM PIN:		OR	CENTRAL SUPPLIER DATABASE No: MAAA
B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE	TICK APPLICABLE BOX] <input type="checkbox"/> Yes <input type="checkbox"/> No		B-BBEE STATUS LEVEL SWORN AFFIDAVIT	[TICK APPLICABLE BOX] <input type="checkbox"/> Yes <input type="checkbox"/> No
[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/ SWORN AFFIDAVIT (FOR EMES & QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]				
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	<input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES ENCLOSE PROOF]	ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES /WORKS OFFERED?	<input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES, ANSWER PART B:3]	
QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS				
IS THE ENTITY A RESIDENT OF THE REPUBLIC OF SOUTH AFRICA (RSA)? <input type="checkbox"/> YES <input type="checkbox"/> NO				
DOES THE ENTITY HAVE A BRANCH IN THE RSA? <input type="checkbox"/> YES <input type="checkbox"/> 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 SIGN A SERVICE LEVEL AGREEMENT.**

2. TAX COMPLIANCE REQUIREMENTS

- 2.1 BIDDER MUST ENSURE COMPLIANCE WITH THEIR TAX OBLIGATIONS.
- 2.2 BIDDER 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 BIDDER MAY ALSO SUBMIT A PRINTED TCS CERTIFICATE TOGETHER WITH THE BID.
- 2.5 IN BIDS WHERE CONSORTIA / JOINT VENTURES / SUB-CONTRACTORS ARE INVOLVED, EACH PARTY MUST

SUBMIT A SEPARATE TCS CERTIFICATE / PIN / CSD NUMBER.

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

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

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

SIGNATURE OF BIDDER:

CAPACITY UNDER WHICH THIS BID IS SIGNED:

(Proof of authority must be submitted e.g. company resolution)

DATE:

18 DECLARATION OF INTEREST

1. Any legal person, including persons employed by the state¹, 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 a price quotation, advertised competitive bid, limited bid or proposal). 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:

.....

2.2 Identity Number:

.....

2.3 Position occupied in the Company (director, trustee, shareholder²):

.....

2.4 Company Registration Number:

.....

2.5 Tax Reference Number:

.....

2.6 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: **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 attached 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.

2.7.2.1 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 / **YES / NO**
shareholders / members or their spouses conduct business with the state
in the previous twelve months?

2.8.1 If so, furnish particulars:

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

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

2.9.1 If so, furnish particulars:

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

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

2.10.1 If so, furnish particulars:

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

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

2.11.1 If so, furnish particulars:

.....

3. Full details of directors / trustees / members / shareholders.

Full Name	Identity Number	Personal Tax Reference Number	State Number / Employee Personal Number

DECLARATION

I, _____ THE _____ UNDERSIGNED
(NAME).....

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

I ACCEPT THAT THE PIC MAY REJECT THE BID OR ACT AGAINST ME SHOULD THIS
DECLARATION
PROVE TO BE FALSE.

.....

.....

Signature

Date

.....

.....

Position

Name of bidder

19 COMPANY INFORMATION

Please complete the following questionnaire:

1. Company Name:

--

2. Other Trading Names:

--

3. Type of Organization: (Public Company ('Limited'), Private Company ('(Pty) Ltd'), Close Corporations ('cc'))

--

4. Physical and Postal Address of the Company:

Postal Code:	Postal Code:

5. Contact Details

Contact Name	
---------------------	--

Contact Number	
Cell Number	
Email Address	
Alternative Contact	
Email Address	
Contact Number	

6. Company Information

Average no. of employees:	
Average annual turnover:	
Type of Enterprise: (e.g. Generic, Qualifying small enterprise, Exempted Micro Enterprise)	
Industry in which the entity operates:	

7. Banking Details

Banker:	
Auditor:	
Year of Establishment:	
Registration number of entity:	
Sector:	

***A letter from your bank with a bank stamp or cancelled cheque must be submitted.**

8. Tax Registration Details:

Income Tax Reference Number:	
VAT Registration Number:	
PAYE Registration Number:	

9. List of Shareholders:

***ID Documents of the Board of directors/members, owners, shareholders or executive committee must be submitted.**

*** CIPC Documents must be attached.**

DECLARATION

Bidder Name: _____

Signature: _____

Designation: _____

I declare that:

- All information provided is true and correct
- The signatory of the bid document is duly authorized
- Documentary proof regarding any bid issue, will, when required be submitted to the satisfaction of the PIC

PIC will upon detecting that:

- The BBBEE status level of contribution has been claimed or obtained on a fraudulent basis;

- Any of the conditions have not been fulfilled act against the bidder.

I understand that:

PIC may:

- Disqualify the bidder from the bidding process;
- Recover all costs, losses or damages it has incurred or suffered as a result of the bidder's conduct;
- Cancel the contract and claim any damages which has suffered as a result of having less favorable arrangements due to cancellation;
- Restrict the bidder, its shareholders and directors or only shareholders and directors who acted on fraudulent basis, from obtaining business from any organ or state for a period not exceeding 10 years after audi alteram partem (hear the other side) rule has been applied; and
- Forward the matter for criminal prosecution

Thus signed and accepted on this _____^{st / nd / rd / th} day of _____ ,

20____ at _____:

Who warrants his / her authority hereto

For and on behalf of:



ANNEXURE A

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

Between

PUBLIC INVESTMENT CORPORATION SOC LIMITED

(Registration Number 2005/009094/06)

("PIC")

AND

(Identity Number / Registration Number: _____)

(Hereinafter referred to as the parties.)

Introduction

1. The parties wish to record the terms and conditions upon which each shall disclose confidential information to the other, which terms and conditions shall constitute a binding and enforceable agreement between the parties and their agents.

2. This agreement shall also bind the parties, notwithstanding the date of signature hereof, in the event that either party shall have disclosed any confidential information to the other party prior to date of signature hereof.

3. For the purposes of this agreement the party which discloses confidential information shall be referred to as “the disclosing party” and the party which receives the confidential information shall be referred to as “the receiving party”.

The Confidential Information

4. "Confidential Information" shall, for the purpose of this agreement include, without limitation, any technical, commercial or scientific information, know-how, trade secrets, processes, machinery, designs, drawings, technical specifications, terms of agreements, details of investment strategies, organisational strategies or structure of either party, products or services offered by either party or any other matter which relates to the business of either party in respect of which information is not readily available in the normal course of business which may come to the knowledge of the other party in whatever form, disclosed to or assessed by either party during the course of his relationship with the other party.

Disclosure of confidential information

5. The disclosing party shall only disclose the confidential information to the receiving party to the extent deemed necessary or desirable by the disclosing party in its discretion.
6. The receiving party acknowledges that the confidential information is a valuable, special and unique proprietary asset to the disclosing party.
7. The receiving party agrees that it will not, during or after the course of their relationship and/or the term of this agreement as described in Clause 17, disclose the information to any third party for any reason or purpose whatsoever without the prior written consent of the disclosing party, save in accordance

with the provisions of this agreement. In this agreement “third party” means any party other than the parties.

8. Notwithstanding anything to the contrary contained in this agreement the parties agree that the confidential information may be disclosed by the receiving party to other related parties on a need-to-know basis; provided that that party takes whatever steps are necessary to procure that such other related parties agree to abide by the terms of this agreement to prevent the unauthorised disclosure of the confidential information to third parties. For purposes of this clause, the receiving party’s other related parties and employees, directors or managers shall be deemed to be acting, in the event of a breach, as that party’s duly authorised agents.

9. The receiving party agrees:

9.1 not to utilise, exploit or in any other manner whatsoever use the confidential information disclosed pursuant to the provisions of this agreement for any purpose whatsoever without the prior written consent of the disclosing party;

9.2 that the unauthorized disclosure of the confidential information to a third party may cause irreparable loss, harm and damage to the disclosing party. Accordingly, the receiving party indemnifies and holds the disclosing party harmless against any loss, claim, harm or damage, of whatever nature, suffered or sustained by the disclosing party pursuant to a breach by the receiving party of the provisions of this agreement.

Title

10. All confidential information disclosed by the disclosing party to the receiving party is acknowledged by the receiving party:

10.1 to be proprietary to the disclosing party; and

10.2 not to confer any rights to the receiving party of whatever nature in the confidential information.

Restrictions on disclosure and use of the confidential information

11. The receiving party undertakes not to use the confidential information for any purpose other than:

11.1 that for which it is disclosed; and

11.2 in accordance with the provisions of this agreement.

Standard of care

12. The receiving party agrees that it shall protect the confidential information disclosed pursuant to the provisions of this agreement using the same standard of care that the receiving party applies to safeguard its own proprietary, secret or confidential information and that the information shall be stored and handled in such a way as to prevent any unauthorised disclosure thereof.

Return of material containing or pertaining to the confidential information

13. The disclosing party may, at any time, request the receiving party to return any material containing, pertaining to or relating to confidential information disclosed pursuant to the terms of this agreement and may, in addition request the receiving party to furnish a written statement to the effect that, upon such return, the receiving party has not retained in its possession, or under its control, either directly or indirectly, any such material.
14. As an alternative to the return of the material contemplated in clause 13 above, the receiving party shall, at the instance of the disclosing party, destroy such material and furnish the disclosing party with a written statement to the effect that all such material has been destroyed. Notwithstanding the aforesaid, the receiving party will be entitled to retain such documents as they are reasonably required to retain in order to fulfil their professional obligation with regard to document retention, imposed on them by the professional body of which they are a member.

15. The receiving party shall comply with a request in terms of this clause, within 7 (seven) days of receipt of such a request.

Excluded confidential information

16. The obligations of the receiving party pursuant to the provisions of this agreement shall not apply to any confidential information that:

16.1 is known to, or in the possession of the receiving party prior to disclosure thereof by the disclosing party;

16.2 is or becomes publicly known, otherwise than as a result of a breach of this agreement by the receiving party;

16.3 is developed independently of the disclosing party by the receiving party in circumstances that do not amount to a breach of the provisions of this agreement;

- 16.4 is disclosed by the receiving party to satisfy an order of a court of competent jurisdiction or to comply with the provisions of any law or regulation in force from time to time; provided that in these circumstances, the receiving party shall advise the disclosing party to take whatever steps it deems necessary to protect its interests in this regard and provided further that the receiving party will disclose only that portion of the information which it is legally required to disclose and the receiving party will use its reasonable endeavours to protect the confidentiality of such information to the greatest extent possible in the circumstances;
- 16.5 is disclosed to a third party pursuant to the prior written authorisation of the disclosing party;
- 16.6 is received from a third party in circumstances that do not result in a breach of the provisions of this agreement.

Term

17. Subject to clause 2 this agreement shall commence upon the date of signature of the last signing party hereto ("the effective date") and shall endure for a period of 12 (twelve) months ("the term") thereafter, or for a period of one year from the date of the last disclosure of confidential information to the receiving party, whichever is the longer period, whether or not the parties continue to have any relationship for that period of time. In the event that the parties extend the term by mutual and written agreement, then the provisions hereof shall endure for a further minimum period of 12 (twelve) months *mutatis mutandis*.

No Solicit

18. Both parties agree that they will not solicit, interfere with, or entice or endeavour to solicit, interfere with or entice away from the other party, any employee or consultant of the other party, or of either parties consultant(s) or sub-contractor, for the duration of this agreement.

Additional Action

19. Each party to this agreement shall execute and deliver such other documents and do such other acts and things as may be necessary or desirable to give effect to the terms and provisions of this agreement.

Breach

20. In the event that the receiving party should breach the provisions of this agreement and fail to remedy such breach within 7 (seven) days from date of a written notice to do so, then the disclosing party shall

be entitled to invoke all remedies available to it in law including the institution of urgent interim proceedings and/or an action for damages.

Amendments

21. No amendment, interpretation or waiver of any of the provisions of this agreement shall be effective unless reduced in writing and signed by both parties.

Enforcement

22. The failure by the disclosing party to enforce or to require the performance at any time of any of the provisions of this agreement shall not be construed to be a waiver of such provision, and shall not affect either the validity of this agreement or any part hereof or the right of the disclosing party to enforce the provisions of this agreement.

Headings

23. The headings of the clauses of this agreement are used for convenience only and shall not affect the meaning or construction of the contents of this agreement.

Representations & Warranties

24. Each party represents that it has authority to enter into this agreement and to do all things necessary to procure the fulfilment of its obligations in terms of this agreement.

Entire agreement

25. This agreement contains the entire agreement of the parties with respect to the subject matter of this agreement and supersedes all prior agreements between the parties, whether written or oral, with respect to the subject matter of this agreement.

Governing law

26. This agreement and the relationship of the parties in connection with the subject matter of this agreement and each other shall be governed and determined in accordance with the laws of the Republic of South Africa.

Submission

27. The parties hereby submit to the non-exclusive jurisdiction of the Northern - Gauteng High Court.

Domicile (Physical Address)

28. Any written notice in connection with this agreement may be addressed:

- 29.1 in the case of PIC to

MENLYN MAINE CENTRAL SQUARE

CORNER ARAMIST AVENUE & COROBAY AVENUE

WATERKLOOF GLEN EXTENSION 2

0181

and shall be marked for the attention of.....;

29.2 in the case of _____ to

and shall be marked for the attention of _____.

30. A party may change that party's address, by prior notice in writing to the other party.

31. If any notice is to be sent by mail, it shall be sent by prepaid registered mail and shall then be deemed until and unless the contrary is proved, to have been received 10 (ten) days after the date of posting.

32. If any notice is sent by telefax, it will be deemed, until and unless the contrary is proved, to have been received on the date recorded on the transmission slip.

33. If any notice is delivered by hand, it will be deemed to have been received on proof of the date of delivery.

Severability

34. In the event of any one or more of the provisions of this agreement being held for any reason to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provision of this agreement, and this agreement shall be construed as if such invalid, illegal or unenforceable provision was not a part of this agreement, and the agreement shall be carried out as nearly as possible in accordance with its original terms and intent.

Signed at on this the day of 2018

Witness signature.

Signature

Duly authorised representative of

Public Investment Corporation SOC Limited

Print name.

Print Name.

Date.

Date.



Signed at _____ on this the _____ day of _____ 2018

Witness signature.

Duly authorised representative of

Print name.

Print Name.

Date.

Date.

ANNEXURE B

Contracting terms and conditions

- Bidder are advised that a valid contract will only come into existence between the PIC and the successful bidder after conclusion of successful negotiations and signature of the Contract by both parties' respective delegated authorities.

Key contractual principles that successful Bidder must note for the final contract are as follows:

- Duration

Contracts will be for a fixed period. There will be no auto-renewals renewals.

- Limitation of Liability

The limitation of liability is subject to negotiation and will be informed by the contract value and risk associated with the contract.

Ownership of Data

The PIC shall retain ownership of the Data and all Intellectual Property Rights in and to all the Data.

Termination of Convenience

PIC requires a clause addressing termination of convenience

Governing Law

The PIC preferred Governing Law of the Contract between the parties is the law of the Republic of South Africa. In the event that the parties cannot agree on South African law, the PIC will accept the law of England.

Warranty

The Successful Bidder warrants that it:

- is authorised to enter into an Agreement and able to perform each of its duties in terms of the Agreement;
- is suitably qualified to provide the Services;
- is registered with the relevant industry body and its employees have the required certification and licences; and
- has public liability insurance cover commensurate with the risks to which it is exposed for the Term of the Agreement. Documentary proof of such insurance cover is to be provided to on or before the Date of Signature.

The Bidder shall provide the Services:

- with due care and skill;
- in accordance with the terms and conditions of this Agreement; and

- in compliance with all applicable laws and regulations.

The Bidder further warrants and guarantees that:

- the Services shall be rendered and executed in a professional manner in accordance with the standards agreed between the Parties and expected in the relevant industry; and
- the personnel tasked with rendering the Services have completed the requisite formal training and have the expertise to execute their functions properly, in particular regarding but not limited to:
- the execution of their Services, having regard for the legal aspects thereof;

Data Storage

The Successful Bidder must disclose where the data is stored. PIC requires data to be stored in the Republic of South Africa or an EU jurisdiction.

Exit Management

If this Agreement is terminated in whole or in part for any reason whatsoever the provisions of the exit management plan agreed (if any) between the Parties shall come into effect and in any event, including where no agreed exit management plan exists, the Supplier shall co-operate fully with the PIC to ensure an orderly migration of the Services to the PIC or, at the PIC's request, a new supplier (an **Orderly Migration**). Without limiting the foregoing, the PIC shall be entitled to require the

Supplier to continue to provide the Services for up to **[6 (six)]** months after the effective date of the termination of this Agreement on the same payment terms if, in the opinion of the PIC, such continuation is required in order to allow for an Orderly Migration. Co-operation by the Supplier shall include (without limitation), at the PIC's election, the provision by the Supplier of such personnel, equipment, resources, software, documentation, training and consultancy as may reasonably be required to enable an Orderly Migration and the return of the PIC's data in the manner, timeframes and a form and format specified by the PIC.