Companies and Intellectual Property Commission

a member of the dti group

## ANNEXURE: "H"

# TERMS OF REFERENCE ("TOR")

**CIPC BID NUMBER:** 09/2023/2023

**DESCRIPTION:** INVITATION TO SUBMIT PROPOSAL FOR THE APPOINTMENT OF AN ICT SERVICES PROVIDER TO PROVIDE MANAGED INFORMATION SECURITY SERVICES

**CONTRACT PERIOD:** FIVE {5} YEARS).

**BID CLOSING DATE:** 19 JULY 2023

**NB: IT IS THE RESPONSIBILITY OF THE PROSPECTIVE BIDDERS TO DEPOSIT TENDERS IN THE CORRECT BOX AND TENDERS DEPOSITED IN WRONG BOXES WILL NOT BE CONSIDERED.**

**THE CIPC TENDER BOX HAS THE FOLLOWING DESCRIPTION: "CIPC TENDER BOX".**

Companies and Intellectual Property Commission

a member of the dti group

**TABLE OF CONTENTS**

## 1. TERMS AND CONDITIONS OF REQUEST FOR TENDER (RFT)

1. CIPC's standard conditions of purchase shall apply.
2. Late and incomplete submissions will not be accepted.
3. Any bidder who has reasons to believe that the RFP specification is based on a specific brand must inform CIPC before BID closing date.
4. Bidders are required to submit an original Tax Clearance Certificate for all price quotations exceeding the value of R30 000 (VAT included). Failure to submit the original and valid Tax Clearance Certificate will result in the invalidation of this RFP. Certified copies of the Tax Clearance Certificate will not be acceptable.
5. No services must be rendered or goods delivered before an official CIPC Purchase Order form has been received.
6. This RFP will be evaluated in terms of the **80/20** system prescribed by the Preferential Procurement Regulations, 2001.
7. The bidder must provide assurance/guarantee to the integrity and save keeping of the information (that it will not amended/corrupted/distributed/permanently stored/copied by the service provider) for the duration of the contract and thereafter. Failure to submit will invalidate the bid proposal.
8. CIPC reserves the right to negotiate with the successful bidder on price.
9. The service provider must ensure that their work is confined to the scope as defined.
10. Travel between the consultant's home, place of work to the DTI (CIPC) vice versa will not be for the account of this organization, including any other disbursements.
11. The Government Procurement General Conditions of contractors (GCC) will apply in all instances.
12. As the commencement of this project is of critical importance, it is imperative that the services provided by the Service Provider are available immediately. Failing to commence with this project immediately from date of notification by CIPC would invalidate the prospective Service Provider's proposal.
13. No advance payment(s) will be made. CIPC will pay within the prescribed period as per the PFMA.
14. **All prices quoted must be inclusive of Value Added Tax (VAT)**
15. **All prices must be quoted in South African Rand**
16. **All prices must be valid for 120 days**
17. The successful Service Provider must at all times comply with CIPC's policies and procedures as well as maintain a high level of confidentiality of information.
18. All information, documents, programmes and reports must be regarded as confidential and may not be made available to any unauthorized person or institution without the written consent of the Commissioner or his/her delegate.
19. The successful bidder must ensure that the information provided by CIPC during the contract period is not transferred/copied/corrupted/amended in whole or in part by or on behalf of another party.
20. Further, the successful bidder may not keep the provided information by way of storing/copy/transferring of such information internally or to another party in whole or part relating to companies and/or close corporation. As such all information, documents, programs and reports must be regarded as confidential and may not be made available to any unauthorized person or institution without the written consent of the Commissioner or his delegate.

21. The service provider will therefore be required to sign a declaration of secrecy with CIPC. At the end of the contract period or termination of the contract, all information provided by CIPC will become the property of CIPC and the service provider may not keep any copy /store/reproduce/sell/distribute the whole or any part of the information provided by CIPC unless authorized in terms of the declaration of secrecy.
22. The Service Provider is restricted to the time frames as agreed with CIPC for the various phases that will be agreed to on signing of the Service Level Agreement.
23. CIPC will enter into Service Level Agreement with the successful Service Provider.
24. **CIPC reserves the right not to award this bid to any prospective bidder or to split the award.**
25. **Fraud and Corruption:**

The Service Provider selected through this Terms of Reference must observe the highest standards of ethics during the performance and execution of such contract. In pursuance of this policy, CIPC Defines, that for such purposes, the terms set forth will be as follows:

i. "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of CIPC or any personnel of Service Provider(s) in contract executions.
ii. "Fraudulent practice" means a misrepresentation of facts, in order to influence a procurement process or the execution of a contract, to CIPC, and includes collusive practice among bidders (prior to or after Proposal submission) designed to establish Proposal prices at artificially high or non-competitive levels and to deprive CIPC of the benefits of free and open competition;
iii. "Unfair trade practices" means supply of services different from what is ordered on, or change in the Scope of Work;
iv. " Coercive practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract;
v. CIPC shall reject a proposal for award, if it determines that the bidder recommended for award, has been engaged in corrupt, fraudulent or unfair trade practices;
vi. **CIPC also reserves the right to terminate this Agreement by giving 10 (ten) business days written notice to the service provider due to any perceived (by CIPC) undue reputational risk to CIPC which CIPC can be exposed to resulting from the service provider or its management/directors being found to be involved in unethical behaviour, whether in its dealings with CIPC or any other business dealings.**
**Note: "Unethical behaviour" includes but not limited to an action that falls outside of what is considered morally right or proper for a person, a profession or an industry**
vii. CIPC shall declare a Service Provider ineligible, either indefinitely or for a stated period of time, for awarding the contract, if at any time it determines that the Service Provider has been engaged in corrupt, fraudulent and unfair trade practice including but not limited to the above in competing for, or in executing, the contract.
viii. The service provider will sign a confidentiality agreement regarding the protection of CIPC information that is not in the public domain.

2. ***COMPLUSORY BID REQUIREMENTS (FAILURE TO COMPLY WITH ALL REQUIREMENTS BELOW WILL IMMEDIATELY DISQUALIFY THE PROPOSAL***

**INSTRUCTIONS FOR THE SUBMISSIONS OF A PROPOSALS**

***SUBMISSION OF ORIGINAL HARD COPY***

a) Bidder's must submit **One (1) original copy (hard printed copy of the technical proposal), this is for record keeping purposes and the USB Only will be used for bids evaluation.**
b) The Bid Document must be marked with the Bidder's Name
c) The Bid documents ***must be signed*** by an authorized employee, agent or representative of the bidder and each and every page of the proposal shall contain the initials of same signatories
d) All pages of the submitted proposal must be numbered.

***SUBMISSION OF USB***

***a) NO DISC WILL BE ALLOWED***
***b)*** **ONE (1) USB *must be submitted, including technical proposal as well as price proposal saved in separate folders;***
***c)*** The USB must be marked with the bidder's name.
d) **The USB must have an index page/ table of contents listed all documents included in the proposal for easy referencing during evaluation (group information in separate folders)**
e) The **USB** must contain the ***exact*** documents/ information submitted in the original copy
f) Bidders to ensure that the information is properly copied in the USB prior submitting to CIPC and that there are no missing pages.
**g) THE USB WILL BE USED FOR EVALUATION HENCE THE BIDDER IS REQUIRED TO ENSURE THAT THE USB CONTAINS ALL INFORMATION.**
**h) CIPC WILL NOT BE HELD LIABLE FOR INCOMPLETE PROPOSALS/ INFORMATION SUBMITTED IN THE USB'S**
i) All pages must be signed; numbered and initial as per the Original copy
j) The USB must be submitted in **PDF format ONLY and must be *read ONLY; NO Passwords Protection***
**k) BIDDERS TO ENSURE THAT USB'S ARE WORKING PRIOR SUBMISSION**
**l) Bidders to ensure that USB 's are not password protected**
**m) IT IS THE BIDDERS RESPONSIBILITY TO VERIFY IF THE USB IS WORKING BEFORE SUBMISSION**
**n) BIDDER'S WITH USB'S NOT OPENING OR PASSWORD PROTECTED WILL BE DISQUALIFIED**

**FAILURE TO COMPLY WITH ALL THE ABOVE MENTIONED REQUIREMENTS WILL IMMEDIATELY INVALIDATE THE BID.**

## 3. *SUBMISSION OF PRICE PROPOSAL*

a) Prospective Bidders must submit a printed hard copy of the Price Proposal in a separate ***SEALED*** envelope. It is important to separate price from the Technical proposal as Price is evaluated at the last phase of the Evaluation.

b) The price envelop must be marked with the bidder's name

*c)* **Bidders to complete Pricing Schedule SBD 3.3 (Annexure "C")-** ***REFER TO ATTACHED SBD FORMS***

*d)* **The total Price** (***Ceiling price)*** must be carried over to **BOTH SBD 3.3 (Pricing Schedule) and SBD FORM 1**: (Invitation for Bids). ***AND COMPLIANCE TO ANNEXURE A ON PAGE 25***

e) The Total Bid Amount will be used for the evaluation of bids therefore it must be inclusive of all costs for the duration of the contract.

*f)* All prices must be VAT inclusive and quoted in South African Rand (ZAR). ***Failure to comply with this requirement will disqualify the bid.***

g) **All prices must be valid for 120 days**

***PLEASE NOTE THAT IT IS COMPULSORY THAT BIDDERS SUBMIT PROPOSAL AS PER THE FOLLOWING***

1. **1 (ONE) ORIGINAL HARD OR PRINTED COPY**
2. **1 (ONE) USB FOR TECHNICAL PROPOSAL AND PRICE MUST BE INCLUDED IN THE SAME USB BUT SAVED IN A SEPARATE FOLDER ("MARKED PRICE PROPOSAL") BIDDERS TO ENSURE THAT USB'S ARE WORKING PRIOR SUBMISSION**
3. **ONE SEALED ENVELOPE FOR PRICE PROPOSAL (INSIDE THERE MUST BE)**

- PRICE SCHEDULE – SBD.33 : **PLEASE TAKE NOTE OF THE CLAUSE IN SBD 3.3 AND ENSURE COMPLIANCE**
- **ALL CONDITIONS OF PRICE FOR EXAMPLE- PRICE FLUCTUATIONS OR PRICES NOT FIRM DUE TO ROE, ETC MUST BE CLEARLY STATED IN SBD 3.3 IN THE SPACE PROVIDED. SEE ANNEXURE "A- PRICING SCHEDULE"**
- SBD1 - INVITATION TO BIDS
- PRICE BREAKDOWN PREFERABLE IN THE BIDDERS LETTERHEAD SIGNED BY AN AUTHORISED REPRESENTATIVE
- BIDDERS TO REFER TO **PAGE 11 AND 19-** REQUIREMENTS ON PRICE PROPOSAL **AND ANNEXURE "A"PAGE 25**

**NB: Bidders must also refer to page 11 of 28 of the Terms of reference under Mandatory Requirements**

***FAILURE TO COMPLY WITH ALL THE ABOVE MENTIONED REQUIREMENTS WILL IMMEDIATELY INVALIDATE THE BID.***

I, the undersigned (NAME)……certify that:

**I have read and understood the conditions of this tender.**

I have supplied the required information and the information submitted as part of this tender is true and correct.

…….. ……..

**Signature** **Date**

***FAILURE TO COMPLY WITH ALL THE ABOVE MENTIONED REQUIREMENTS WILL IMMEDIATELY INVALIDATE THE BID.***

## 1. Background

The Companies and Intellectual Property Commission (CIPC) requires a comprehensive managed information security services towards the protection of its computing assets. The managed information security services initiative encompasses the following broad streams i.e., Network Security, Data Security, Access Control, Application Security, People Security, Endpoint Security and Governance Risk and Compliance. CIPC seeks the managed information security services that are in South Africa that can be both remote and physically accessed. The managed information security service must be integrate-able with CIPC environment, remotely and physically managed.

## 2. Purpose

The primary aim of these terms of reference is to provide information involved with the advancement of the managed information security services at the CIPC. It will form the basis for effective decision making about the identified programme streams such as the:

a. **Network Security** - Managed Security Operations Centre (SOC), Extended Detection and Response (XDR), Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), Web Gateway and Next Generation Firewall (NGFW).
b. **Data Security** - Data Loss Prevention (DLP), Database Activity Monitor (DAM), Data Masking, and Database Encryption.
c. **Access Control** - Privilege Access Management (PAM), Identity and Access Management (IAM), Multi-factor Authentication (MFA)
d. **Application Security** – Application Code Review, Secure APIs and Third-Party Data Sharing.
e. **People Security** – Cybersecurity Awareness, Training and Education
f. **Endpoint Security** - Threat Hunting and Threat Intelligence, Managed Detection and Response (MDR) including operations and monitoring, Incidence Response, and Vulnerability Management
g. **Governance Risk and Compliance**

## 3. Business Objectives

The Managed Information Security Services must enable or assist CIPC in achieving the following business objectives (the order of the list does not reflect the importance or the priority of the objectives):

3.1.1 The service must be capable of supporting CIPC's current needs and be able to adapt to CIPC's future information security needs as the evolving threat landscape.

3.1.2 Provides a Managed Security Operations Centre (SOC) that monitors and manages each CIPC's installed base and reports infections and other alerts as configured.

3.1.3 Provides a platform that integrates and interoperates with other information security systems and tools (existing and future) to improve CIPC's overall information security posture and enable all facets of CIPC's business.

3.1.4 Prevents cyber breaches by pre-emptively blocking known and unknown ransomware, malware, exploits, and zero-day threats.

3.1.5 Provides administrative access that is role based, allowing CIPC staff to have appropriate access based on their assigned role.

3.1.6 Enables and protects all CIPC users as they safely perform their daily business activities using web-based technologies and local resources without becoming a hindrance or negatively affecting user experience with CIPC's systems.

3.1.7 Must be able to seamlessly integrate within CIPC's/IT business activities and practices and not require a major change to the existing CIPC and IT operations.

3.1.8 Must improve Enterprise Security posture, enable CIPC to utilize internet-based information, and services safely.

3.1.9 Provides excellent detection and protection services to the CIPC's systems to improve the CIPC's responsiveness to changing business conditions.

3.1.10 Improves the CIPC's systems' security, availability, resiliency, and capacity without being cost prohibitive.

3.1.11 Provides the CIPCs with a deeper understanding of the granular usage of the system application visibility and control.

3.1.12 Adhere to the CIPC's information security plans to ensure all security guidelines and standards are achieved.

3.1.13 Support CIPC System's policies related to safe data handling, data security, and acceptable technology use.

## 4. Solution Vision

To acquire a Managed Information Security Services that will deliver the business objectives as outlined above. The service must be efficiently managed, and monitored to keep the CIPC's systems secure in today's changing threat landscape. The Managed Information Security Services must seamlessly integrate with the CIPC systems, to prevent any disruption to CIPC business.

## 5. Current Environment

Below is the list of devices that are currently supported by the CIPC from which the Managed Information Security Service is sourced to support the CIPC:

| Devices | Number |
|---|---|
| Workstations / Laptops | 483 |
| **Microsoft Windows Servers OS** | |
| Server 2003 and 2003 R2 | 1 |
| Server 2008 and 2008 R2 | 2 |
| Server 2012 and 2012 R2 | 108 |
| Server 2016 | 54 |
| Server 2019 | 26 |
| Hyper-V Hosts | 10 |
| Virtual | 161 |
| VMWare VSphere Hosts | 10 scalable |
| Linux Servers | |
| New Production | 16 |
| Old Production | 3 |
| **2X External Firewall** | |
| 10Gbps of firewall throughput for HTTP and appmix transactions.<br>6 Gbps of IPsec VPN throughput.<br>1 000 000 sessions | |
| **2X Internal Firewall** | |
| 38Gbps of firewall throughput for HTTP and appmix transactions.<br>20Gbps of IPsec VPN throughput.<br>3 000 000 sessions | |
| **2X Web Applications Firewalls** | |
| **Aruba NAC Solution** | |
| **Mimecast Mail Security** | |
| | |
| **Trellix Endpoint Security Solution** | |
| 2 x McAfee Network Security Manager (NSM) | |
| 650 x MVISION Protect Plus EDR for Endpoint | |
| 650 x Skyhigh ShadowIT 1YrBZ SUB for BUSINESS | |
| 650 x Skyhigh ShadowIT 1:1 BZ | |
| 650 x Trellix EDR&EPP UPGD (DE) 1:1BZ | |
| 650 x Complete Data Protection for BUSINESS | |
| 350 x McAfee Cloud Workload Security Advanced for BUSINESS | |
| 15 x McAfee Datacenter Sec Suite Database | |
| 1 x McAfee Network Security Platform for BUSINESS | |
| 1 x McAfee Network Security Platform for BUSINESS | |
| 1 x McAfee Network Security Platform for BUSINESS | |
| 1 x McAfee Network Security Platform for BUSINESS | |
| 650 x McAfee Total Protection for DLP for BUSINESS | |
| 650 x Web Protection Suite 1:1 BZ | |
| 650 x McAfee Web Protection Suite for BUSINESS | |
| 1 x McAfee Web Gateway SAME BUSINESS DAY UPGRADE | |
| 1 x McAfee Web Gateway SAME BUSINESS DAY UPGRADE | |
| 1 x ATD-6000 MFE Adv Threat Def 6000 Standard HW | |

| | |
|---|---|
| 650 x Complete Data Prtxn P:1BZ[P+]CompUpg | |
| 650 x MFE Complete EP Protect Ent P:1 BZ [P+] | |
| 15 x Datacenter Sec Suite DbaseP:1BZ [P+] | |
| 1 x MFE DLP 5500 Copper Appliance | |
| 1 x MFE DLP 5500 Copper Appliance | |
| 1 x MFE DLP 5500 Copper Appliance | |
| 1 x MFE DLP 5500 Copper Appliance | |
| 1 x MFE DLP 5500 Copper Appliance | |
| 350 x MFE Server Security Suite Adv P:1BZ[P+] | |
| 650 x EP Threat Def and Resp P:1 BZ[P+] | |
| 650 x Total Protection for DLP SW P:1 BZ | |
| 1 x MFE Web Gateway 5000 Appl-C | |
| 1 x MFE Web Gateway 5000 Appl-C | |
| 650 x MFE Web Reporter Premium P:1 BZ | |
| 1 x MFE Net Sec IPS-NS9100 Appliance | |
| 1 x MFE Net Sec IPS-NS9100 Appliance | |
| 1 x Skyhigh SWG 5000 Appl-E | |
| 1 x Skyhigh SWG 5000 Appl-E | |
| 600 x- MFE Total Protection fr SecBus P:1BZ[P+] | |
| 1 x MFE Network Sec 2700 Sensor Appl HW | |
| 1 x Network Sec Starter Manager P:1 BZ | |
| 100 x MFE Total Protection fr SecBus P:1BZ[P+] | |
| 700 x MFE Email & Web Sec Virt Ap SW P:1BZ[P+] | |
| **Cortex XDR Pro Suite** | |
| | |

## 6. Solution Requirements

The purpose of this bid is to appoint a suitably qualified Information Security Service Provider to provide Managed Information Security Services and related support services for a period of 5 years. The services to be provided must be within the defined service standards, ethics, processes, and industry best practice. The proposed services must be reliable and highly available and be able to integrate with all CIPC's ICT infrastructure equipment, applications and services.

### 6.1.1. Cyber Security Monitoring, Security Event Management and Security Operations Centre (SOC)

I. Provide a Security Operations Centre (SOC) service

II. The SOC must collect logs from:

- All information security systems (such as firewalls, active directory, endpoint protection, IPS, e-mail security systems)
- All Windows servers
- All Linux servers

III. The SOC service must be delivered as a Cloud service.

IV. All components of the SOC service must be delivered from within the borders of South Africa.

V. The SOC service must provide:

- Analytics (analyse events to produce incidents)
- Monitoring (24x7 monitoring required)
- Alerts (e-mail, SMS or phone)
- Incident management (track and escalate incidents)
- Categorisation (type of incident and why it is being raised)
- Threat hunting (continuously look for and implement new indicators of attack)
- Prioritisation of incidents (different severities which must be measured by an SLA)
- Standard operating procedures for all the functions within the SOC.
- Investigation into suspicious activities, ensuring that potential security incidents are correctly defended, identified, analysed, investigated and escalated to keep the infrastructure secure.
- Coordinate response to threats through managing other team members effectively.

(vi) The SOC must provide an interactive dashboard that must:

- Present incidents in a simple view
- Provide categorisation of incidents
- Prioritise incidents.
- Provide recommended actions to incidents.
- Allow for incidents to be closed via the dashboard.

(vii) The SOC must enrich the log data with at least 5 threat feeds provided by the SOC.

(viii) The SOC must provide monthly reports indicating the activities and incidents of the previous month. These must be presented across an on-line session.

(ix) The SOC must be ISO 27001 or SANS 27001 certified

(x) At least 2 references must be provided for delivering a fully managed SOC service

(xi) All licensing for the SOC must be included

### 6.1.2. Cyber Security Governance Risk and Compliance Management Services

I. Risk assessment and planning.
II. Tracking of metrics.
III. Investigation of anomalies.
IV. Mitigation and remediation of potential threats and well-known security violations.
V. Monitoring and responding to industry regulatory trends.
VI. Integration of assurance initiatives across the organisation.
VII. Mapping operational activities to recognised frameworks and standards.

### 6.1.3. Vulnerability Tracking and Management

I. Perform quarterly vulnerability scans as follows:
   - One scan per quarter must be performed against the Internet facing infrastructure.
   - The other scan per quarter must be performed against the entire internal network.

II. Present the scan results on dashboards accessible by the CIPC. These must show critical and high vulnerabilities as well as easily exploitable hosts.

III. Provide monthly reports indicating which hosts and vulnerabilities should be prioritised.

IV. All licensing must be included.

V. Perform remediation of all identified vulnerabilities (this includes vulnerabilities not addressed by patch management).

### 6.1.4. Patch Management

i. Ensure that every system and application is up to date with the latest versions of operating systems (Microsoft Windows, Linux, etc.), database solutions and third-party applications (Adobe Flash, Acrobat Reader or Internet

browser) released by vendors. The bidder must provide a single software solution to patch Microsoft Windows, Linux, etc. operating systems and third-party applications.

ii. Keep application software and Operating Systems (OS) up to date with the most recent security patches to protect the CIPC from malware and ransomware attacks.
iii. Keep systems up to date with the latest security patches from a single, easy-to-use web console.
iv. Support operating systems, Adobe products, Java, and more.
v. Auto-approve patches for specific programs based on severity levels.
vi. Provide clear, complete and transparent reports over patch statuses to fix issues as they arise.
vii. Schedule patching windows so you can update software without disrupting critical productive times.
viii. Manually approve patches in batch across sites, networks, servers, and workstations.

### 6.1.5. Risk Assessment and Cyber Awareness

i. Provide an assessment approach and methodology link to cybersecurity best practise to help identify, evaluate, and minimise risks to the IT environment that supports the CIPC's mission critical systems.
ii. Provide system and application users with security awareness training. This training should cater for approximately 500 users.
iii. Conduct an annual Information Security risk assessment to determine the extent of the potential threats and the risks within the environment.
iv. During risk assessment process, identify appropriate controls to reduce or eliminate Information Security risks and measure the CIPC security posture against global cybersecurity industry best practises.

(v) Continuously and consistently document vulnerability sources that should be considered in a thorough vulnerability analysis when conducting the annual risk assessment.

### 6.1.6. Connectivity

I. The successful service provider must have two independent sites, both of which must be located within the borders of South Africa.
II. Secure VPN connections must be established to each of these sites across the Internet.
III. All log data and management activities must be conducted across these links. The links will terminate at the CIPC Data Centres. It is required that connectivity between these two sites must be available 24*7*365 days for the proposed services.
IV. Service providers are required to indicate how the proposed solution will be provisioned by means of a detailed architecture diagram and description of how this will be managed.

### 6.1.7. Project Management Services

The successful service provider must provide project management services such as Project Management, Project coordination, Project administration and all other relevant project team members/specialists. The successful service provider will also be expected to lead and facilitate technical discussions during the planning, design, and implementation of the proposed solution up to the operation stage. The successful service provider will also be expected to ensure that the following requirements are fulfilled:

I. establish a master project plan with project timelines.
II. The project manager should have experience in managing similar project(s). The experience of the project manager must be elaborated with a detailed CV.
III. provide Standard Operating Procedures for the deployed solutions.

After the services have been handed over to operations, the service provider will also be expected to provide project management services as and when project related services are required at no additional cost to the CIPC. The amount included in the cost model for the projects is the ceiling amount allocated by the CIPC for the duration of the contract and is not an amount payable or accrued to the successful bidder. It is therefore not guaranteed that the full amount will be utilised during the contract period.

## 7. Implementation Requirements

The first phase which, involves planning, installation, configuration, and deployment of the selected solution to a subset of systems, must be completed by a date arranged with the BISG leadership after the RFP is awarded. The selected bidder is expected to have the overall responsibility for the successful deployment and operation of the selected enterprise security solution.

## 8. Bidder's Commitment

The following work/commitment is expected from the selected bidder:

8.1 Provides deployment assistance (i.e., planning, best practices, etc.) to the IT staff.
8.2 Configure the cloud-based and local administrative console to the CIPC's requirements and specifications.
8.3 Timely resolve deployment and operational issues as they arise during and after the deployment.
8.4 Provides training and continuous knowledge transfer to the identified IT staff, which will help to increase their understanding of the solution during project implementation.

8.5 Integrate and interoperate with the existing solutions (such as, NAC, PAM, Firewall, IDS/IPS, Web and Email Gateways etc…) and future tools for information security (such as, Security Orchestration, Automation and Response (SOAR), Network security monitoring, Encryption, Pen Test, Web Vulnerability Scanning etc…), and Service Desk centralised systems.

8.6 Provides periodic functional and feature improvements to the solution and administrative console to increase the effectiveness of its solution.

8.7 Provides the professional services that are necessary to satisfy the requirements contained within the RFP.

## 9. Testing, Staging, and Deployment

9.1 Bidders are required to submit the complete project plan and action steps specifying execution items.

9.2 The bidder is required to provide product roadmap (coming features) and its associated delivery date.

9.3 The bidder must provide a summary of known outstanding issues with the current version of the proposed solution and expected resolutions.

9.4 Bidders must work in such a manner that CIPC business is not negatively affected in any way.

9.5 It is the bidder's responsibility to successfully deploy and integrate the procured solution into CIPC systems (install, configure, and integrate where it is appropriate) as per CIPC business schedule and requirements.

9.6 Configure the management console to provide required functionality outlined in this RFP.

9.7 Describe any monitoring tools or plug-ins (i.e., Vantage plug-ins) that is available to monitor the system.

## 10. Training and Support

The bidders must describe how, and from where they will provide necessary support and the period during the acceptance periods. The bidders should specify whether they could provide on-site support in cases of an emergency. The bidders must include a proposed Service Level Agreement (SLA), which contains support levels, priority levels, response times, and contact methods.

## 11. Timeframes

The service providers should indicate through a project plan how they will design, implement and support the solution over a **5 Years' period.**

***PLEASE NOTE***: CIPC reserves the right to procure only selected components, firewall layers or services based on the solution proposed.

## 12. Reporting

The contracted bidder's account manager will report to the CIPC Process Owner or his delegate.

## 13. Proprietary Rights

The proprietary right with regard to copyright, patents and any other similar rights that may result from the service rendered by the resource belong to CIPC.

- The final product of all work done by the resource, shall at the end of service period, be handed over to CIPC.
- The resource may not copy documents and/or information of the relevant systems for any other purpose than CIPC specific.

## 14. Indemnity / Protection / Safeguard

- The resources safeguard and set CIPC free to any losses that may occur due to costs, damage, demands, and claims that is the result of injury or death, as well as any damage to property of any or all contracting personnel, that is suffered in any way, while delivering a service to CIPC.
- The resources safeguard and set CIPC free to any or all further claims for losses, costs, damage, demands and legal expenses as to the violation on any patent rights, trade marks or other protected rights on any software or related data used by the resources.

## 15. Government Safety

- The resources attention is drawn to the effect of government Safety Legislation. The resources must ensure (be sure) that relevant steps are taken to notify the person(s) of this solution.
- The resource must at all times follow the security measures and obey the rules as set by the organization.

## 16. Quality

- The Senior Manager: Information Assurance will subject the quality and standard of service rendered by resources to quality control.
- Should CIPC, through the Senior Manager: Information Assurance, be of the opinion that the quality of work is not to the required level, the service provider will be requested to provide another resource. The service provider will carry the cost related to these changes.

## 17. COSTING

- **Please refer to ANNEXURE A PAGE 25 for the details below on how pricing should be submitted**
- Prospective bidders must submit a bill of quantities clearly indicating the unit costs and any other costs applicable. The onus is upon the prospective bidders to take into account ***all costs for the duration of the contract period and to CLEARLY indicate the price***
- **Note: Service providers will be responsible for all costs e.g. Transportation for ALL activities associated with this bid. PLEASE NOTE**: CIPC reserves the right to procure only selected components, firewall layers or services based on the solution proposed.
- **NB The total price must be carried over to the pricing schedule and will be used to evaluate the bids. Prices must be firm for the duration of the project. PRICE CARRIED OVER TO SBD FORM 3.3 AND SBD FORM 1 MUST INCLUDE ALL COSTS FOR THE DURATION OF ALL PERIOD STATED ABOVE UNDER PRICING. FAILURE TO COMPLY WITH THIS REQUIREMENT SHALL IMMEDIATELY INVALIDATE THE BID.**

## 18. SPECIAL CONDITIONS

i. The bidder must provide assurance/guarantee to the integrity and safe keeping of the information (that it will not amended/corrupted/distributed/permanently stored/copied by the service provider) for the duration of the contract and thereafter;

ii. CIPC reserves the right to negotiate with the successful bidder on price;

iii. Travel between the consultant's home, place of work to the **dti Campus (**CIPC) will not be for the account of CIPC, including any other disbursements unless agreed to in writing by CIPC prior to the expense being incurred;

iv. Government Procurement General Conditions of Contract (GCC) as issued by National Treasury will be applicable on all instances. The general conditions are available on the National Treasury website (www.treasury.gov.za);

v. No advance payment will be made. Payment would be made in terms of the deliverables or other unless otherwise agreed upon by CIPC and the successful bidder. CIPC will pay within the prescribed period according to PFMA;

vi. The price quoted by the prospective service provider must include Value Added Tax (VAT);

vii. The successful bidder must at all times comply with CIPC's policies and procedures as well as maintain a high level of confidentiality of information;

viii. The successful bidder must ensure that the information provided by CIPC during the contract period is not transferred/copied/corrupted/amended in whole or in part by or on behalf of another party;

ix. Further, the successful bidder may not keep the provided information by way of storing/copy/transferring of such information internally or to another party in whole or part relating to companies and/or close corporation;

x. As such all information, documents, programs and reports must be regarded as confidential and may not be made available to any unauthorized person or institution without the written consent of the Commissioner and/or his/her delegate;

xi. The service provider will therefore be required to sign a Declaration of Secrecy with CIPC. At the end of the contract period or termination of the contract, all information provided by CIPC will become the property of CIPC and the service provider may not keep any copy /store/reproduce/sell/distribute the whole or any part of the information provided by CIPC unless authorized in terms of the Declaration of Secrecy;

xii. The Service Provider (successful bidder) will be required to sign a Service Level Agreement with CIPC prior to the commencement of the contract; and

xiii. Compliance with PFMA regulations in terms of the safeguarding of assets and adequate access control must be guaranteed. Assets include all infrastructure, software, documents, backup media and information that will be hosted at the Offsite ICT Recovery Site. These security measures must be specified in the SLA.

xiv. As the commencement of this contract is of critical importance, it is imperative that the prospective Service Provider has resources that are available immediately. Failure to commence with this contract immediately from date of notification by CIPC could invalidate the prospective Service Provider's proposal.

xv. The Service Provider shall be required to provide training & skills transfer for the services as per paragraph 3 of this document.

xvi. Service Provider shall provide CIPC with all the license documentation that CIPC is entitled to as per the costing of the licenses.

xvii. The Service Provider shall be required to provide training & skills transfer for the services as per paragraph 3 of this document.

xviii. Bidders shall be subjected requested to demonstrate all claims made in the proposal.

xix. The resources that a bidder supply will be subjected to an assessment results which will determine the suitability of the service provider to implement against the assignment of the ToR. Failure to provide suitable candidates will lead to cancellation of award of the tender.

xx. CIPC reserves the right not to make this appointment

## 19. EVALUATION PROCESS (Criteria)

The evaluation process will be done in accordance with the following criteria:
Bids will be evaluated in accordance with the **80/20** preference point system contemplated in the Preferential Procurement Policy Framework Act (Act 5 of 2000).

### 19.1 . Evaluation (Phases)

**The evaluation will be completed in 3 phases:**

**Phase 1: Compliance to minimum requirements**

**Phase 2: Compliance to Bid Specification (FROM PAGE 20)**

**Phase 3: Functional Evaluation**

**Phase 4: Pricing and Preferential Procurement policy**

## PHASE 1: COMPLIANCE TO MINIMUM REQUIREMENTS AND MANDATORY REQUIREMENTS

During Phase 1 all bidders will be evaluated to ensure compliance to minimum document requirements. Without limiting the generality of the CIPC's other critical requirements for this Bid, bidder(s) ***must submit the documents*** listed in the **Table** below. All documents must be completed and signed by the duly authorized representative of the prospective bidder(s). During this phase Bidders' response will be evaluated based on compliance with the listed administration and mandatory bid requirements. All bidders that comply with the minimum requirements will advance to Phase 2.

| Item No | Document that must be submitted | Compliance provide ANSWER: Yes /No | Non-submission may result in disqualification |
|---|---|---|---|
| 1. | **Invitation to Bid – SBD 1** | | Complete and sign the supplied pro forma document. |
| 2. | **Tax Status – SBD1** | | a) Bidders must submit **Tax Clearance Certificate (TCC) PIN**<br>b) **The TCS PIN** will be used for the verification of tax compliance status a Bidder |
| 3. | **Declaration of Interest –SBD 4** | | Complete and sign the supplied pro forma document. |
| 4. | **Preference Point Claim Form – SBD 6.1** | | Non-submission will lead to a zero (0) score on BBBEE |
| 5. | **Declaration of Bidder's Past Supply Chain Management Practices – SBD 8** | | Complete and sign the supplied pro forma document. |
| 6. | **Certificate of Independent Bid Determination – SBD 9** | | Complete and sign the supplied pro forma document. |
| 7. | **Registration on Central Supplier Database (CSD** | | The Service Provider is encouraged to be registered as a service provider on the Central Supplier Database (CSD). Visit https://secure.csd.gov.za/ to obtain your. Vendor number.<br>Submit PROOF of registration on the Central Supplier Database (CSD Report)<br>**SUBMIT SUPPLIER NUMBER AND UNIQUE REFERENCE NUMBER** |
| 8. | **NB: Pricing Schedule:**<br><br>**Compliance to PAGE 06 AND 25- ANNEXURE A**<br><br>**REFER TO PAGE 5 TO 6 and 25**<br>***FAILURE TO COMPLY WITH THIS REQUIREMENT SHALL IMMEDIATELY DISQUALIFY A BIDDER.*** | | • Submit full details of the Price Proposal in a separate **SEALED** envelope.<br>• Price must be carried over to **BOTH SBD 3.3 (Pricing Schedule) and SBD FORM1**: (Invitation for Bids). *The Total Bid Amount (**CEILING AMOUNT**) will be used for the evaluation of bids therefore it must be inclusive of all costs for the duration of the contract)*<br>***FAILURE TO COMPLY WITH THIS REQUIREMENT SHALL IMMEDIATELY DISQUALIFY A BIDDER.*** |
| 9 | **IMPORTANT: *SUBMISSION OF USB***<br><br>**REFER TO PAGE 5 OF 17** | | 1. Bidders must submit a USB with their proposal- 1 copy of the original document<br>2. USB to be submitted in pdf format and to be read only<br>3. All documents to be signed and bidders initial each page<br>***FAILURE TO COMPLY WITH THIS REQUIREMENT SHALL IMMEDIATELY DISQUALIFY A BIDDER.*** |
| 10 | **Bidders shall submit a letter of Accreditation ISO 27001 or SANS 27001 certification provided by an accredited service provider) –**<br>**Failure to submit will render your bid invalid.**<br><br>***IMPORTANT –NON COMPLIANCE WILL IMMIDIATELY INVALIDATE THE BID***<br>• The ISO 27001 Certificate must be valid and belong to the bidding company. –<br>• If the ISO27001 or SANS 27001 certificate is not belonging to the bidding company, a letter from the Certified/ Reseller company confirming permission to use the certification, should accompany the certificate.<br>• A bidder will be disqualified should a submitted certificate is not from a Reseller of their solution with a letter of approval to use the certification.<br>• The letter of approval by the Reseller must be in bidding company's name signed and dated by the authorized representative.<br>**FAILURE TO SUBMIT WILL RENDER YOUR BID BEING DISQUALIFIED** | | **The ISO 27001 or SANS 27001 Accreditation must be submitted in order to proceed to the next phase** (phase 2).<br>1. Bidders to ensure certification are addressing the requirements stated.<br>2. All bidders are required to comply with this requirement.<br>3. The certification must be signed dated by authorized representative<br>4. It should state expiry date or validity<br>5. The letter of approval to use the Reseller's ISO 27001 or SANS 27001 certification for the proposed solution must be in the bidding company's name and must be signed and dated by the authorized representative<br>6. Non- compliance with these requirements will immediately disqualify the bid.<br><br>**FAILURE TO COMPLY AND SUBMIT THE REQUIRED DOCUMENTATION WILL RENDER YOUR BID INVALID** |

**ALL BIDDERS THAT COMPLY WITH THE MINIMUM REQUIREMENTS WILL ADVANCE TO PHASE 2. SPECIFICATION COMPLIANCE**

Companies and Intellectual Property Commission
a member of the dti group

## PHASE 2: COMPLIANCE TO BID SPECIFICATION

***BIDDERS TO NOTE:***

1. Bidders are required to comply to the specification below as well as address the requirement of the terms of reference.
2. Bidder must attach evidence or proof for all the capabilities below.
3. The evidence will be used for evaluation.
4. Bidders who fail to demonstrate/attach/provide evidence will not proceed to Phase 3 –functional evaluation.
5. The bidders must **fully comply** to answer everything, with nothing left unanswered as failure will disqualify the bidder to proceed to Phase 3 – functional evaluation.
6. Bidders must indicate **exactly to the page** where it shows that they comply as failure will disqualify the bidder to proceed to Phase 3 – functional evaluation.
7. Bidders must **not direct CIPC** to any other tender as doing so will disqualify the bidder from proceeding to Phase 3 – functional evaluation.
8. Bidders must provide CIPC with a **relevant proposal** that indicates how the prospective bidder will deliver the product / service / proposed solution.
9. Bidders must capture how licensing, support and maintenance are going to be provided.
10. Bidders must respond to the Bill of Material (BOM) for the current solutions that exists at CIPC.

### TECHNICAL REQUIREMENTS

The solution must have the capability to support the below solutions:

| Technical Requirement | Notes | Status (Comply/Not Comply) | Evidence (Page #) State page number where # evidence/proof is placed / attached |
|---|---|---|---|
| **Endpoint Security Management** | BOM provided | | |
| NB: Currently exists at CIPC. Requirement is compliance with the BOM including licensing, support and maintenance for 5 years | | | |
| **Endpoint Encryption** | BOM provided | | |
| NB: Currently exists at CIPC. Requirement is compliance with the BOM including licensing, support and maintenance for 5 years | | | |
| **Web Gateways** | BOM provided | | |
| NB: Currently exists at CIPC. Requirement is compliance with the BOM including licensing, support and maintenance for 5 years | | | |
| **Database Security** | BOM provided | | |

| | | | |
|---|---|---|---|
| NB: Currently exists at CIPC. Requirement is compliance with the BOM including licensing, support and maintenance for 5 years | | | |
| **Extended Detection and Response** | BOM provided | | |
| NB: Currently exists at CIPC. Requirement is compliance with the BOM including licensing, support and maintenance for 5 years | | | |
| **Privilege Access Management** | New Requirement | | |
| NB: New requirement including the solution's licensing, support and maintenance for 5 years | | | |
| **Vulnerability Management** | New Requirement | | |
| NB: New requirement including the solution's licensing, support and maintenance for 5 years | | | |
| **Application Security (Code Review)** | New Requirement | | |
| NB: New requirement including the solution's licensing, support and maintenance for 5 years | | | |
| **Cybersecurity Awareness and Training Program** | License, Support and Maintenance Required | | |
| NB: Currently exists at CIPC. Requirement is compliance with the BOM including licensing, support and maintenance for 5 years | | | |
| **Email Security** | Integration with SOC | | |
| NB: Currently exists at CIPC. Requirement is integration with SOC | | | |
| **Network Access Control** | Integration with SOC | | |
| NB: Currently exists at CIPC. Requirement is integration with SOC | | | |
| **Next Generation Firewall & WAF** | Integration with SOC | | |
| NB: Currently exists at CIPC. Requirement is integration with SOC | | | |

**BOM 1**

| QTY | DESCRIPTION | SERIAL NUMBER |
|---|---|---|
| 750 | PAN-XDR-ADV-EP | 220980000 |
| | Cortex XDR Pro for 1 endpoint, includes | |
| | 30 days of data retention and standard | |
| | success | |
| 750 | PAN-XDR-HOST-INST | 220980000 |
| | Host Insights add-on for Cortex XDR | |
| 100 | PAN-XDR-FRNS | 220980000 |
| | Annual Forensics add-on for Cortex | |
| | XDR | |
| 1 | PAN-XDR-PREM-SUCCESS | 220980000 |

| | | |
|---|---|---|
| | Cortex XDR Premium Success | |
| 10 | PAN-XDR-ADV-1TB | 220980000 |
| | Cortex XDR Pro for 1 TB, includes 1TB | |
| | of Cortex Data Lake and standard | |
| | success | |
| 1 | PAN-UNIT42-XMDR & PAN-CONSULT-XDR-U42-OPT-DFIR-S | 220980000 |
| | Palo Alto Networks eXtended Managed | 17457 |
| | Detection and Response service for | |
| | XDR Pro EP, Cloud and for XDR Pro TB | |

**BOM 2**

| Product Name | Charge Type | Trellix/SH SKU | Channel SKU | Quantity |
|---|---|---|---|---|
| Trellix Threat Intelligence Exchange | Perpetual License | TIECDE-AA | TIECDE-AA-FA | 650 |
| ProtectPLUS Business Software Support | Support Fee | CDBYFM-AA | CDBYFM-AA-FA | 650 |
| ProtectPLUS Business Software Support | Support Fee | DCDYCM-AA | DCDYCM-AA-FA | 15 |
| Business Software Support | Support Fee | TDLYCM-AA | TDLYCM-AA-AA | 650 |
| Deployment Consulting Daily - Prepaid | Services Fee | MD-DEPLOY-DYPP | MD-DEPLOY-DYPPA | 50 |
| Business Software Support & Onsite 4 Hour Same Day 24x7 Hardware Support | Support | WBG5000ESDA | WBG5000ESDA | 1 |
| Business Software Support & Onsite 4 Hour Same Day 24x7 Hardware Support | Support | WBG5000ESDA | WBG5000ESDA | 1 |
| Skyhigh Web Protection Suite 2– WPS2 | Subscription License | WP2ECE-AA-FA | WPMA-3JB2-7RLL-K7V6 | 650 |
| Skyhigh CASB for Shadow IT | Subscription License | C02ECE-AA-AA | C02ECE-AA-AA | 650 |

**PLEASE NOTE**: CIPC reserves the right to procure only selected services based on the solution proposed, e.g., CIPC may elect to acquire the installation and implementation from one supplier, and the ongoing support from another.

**PROPOSALS MUST INCLUDE:**

a) License, support and maintenance of the **existing** (BOM 1 and 2 above) solutions
b) License, support and maintenance of the **new** solutions

***FAILURE TO COMPLY WITH THE ABOVE -MENTIONED REQUIREMENTS FOR PHASE 2 SHALL IMMEDIATELY DISQUALIFY A BIDDER TO PROCEED TO PHASE 3 FUNCTIONAL EVALUATION***

Companies and Intellectual Property Commission

## PHASE 3: FUNCTIONAL EVALUATION AND COMPLIANCE TO SPECIFICATION

**All bidders that advance to Phase 2 will be evaluated by a panel to determine compliance to the functional requirements of the bid.**

***The functional evaluation will be rated out of 100 points and will be determined as follows:***

| No | EVALUATION CRITERIA | Rating | | | | | Weight |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | |
| 1. | **Demonstrate Proposed Architecture Solution**<br>Design & implement the architected solution.<br>Build meaningful dashboard, charts and graphs as per CIPC's requirements.<br>Build custom correlation rules as per CIPC's requirement.<br>Create alerts as required by CIPC.<br>Implement as per CIPC requirements.<br>Training as well as knowledge transfer to CIPC ICT Staff in terms of<br>Technical training certification – classroom training and certification<br><br>***Ratings to be awarded as follows:***<br>1. ***Score 1=*** *No proposed designs of architecture solution provided*<br>2. ***Score 2=*** *Insufficient proposal with no architecture implementation solution (partly addressed) no integration with CIPC's entire Environment*<br>3. ***Score 3=*** *Designs and Architect a solution as per OEM best practices and Integration with CIPC's entire Environment.*<br>4. ***Score 4=*** *Designs and Architect a solution as per OEM best practices, training and certification, knowledge and skills transfer plan and Integration with CIPC's entire Environment.*<br>5. ***Score 5=*** *Designs and Architect a solution as per OEM best practices, knowledge and skills transfer plan, Hardened Operating System deployed as a multi-role appliance for granular, distributed functionality and enhanced scalability to meet the demands of CIPC environment, create alerts and customization of rules required.*<br>**NB: Training and knowledge transfer to three (3) CIPC resources** | | | | | | **30** |
| 2. | **Project Plan**<br><br>Methodology and Approach on how the bidder will achieve the following<br>Cyber Security Compliance Management Services<br>Vulnerability Tracking and Management<br>Patch Management<br>Risk Assessment<br>Connectivity<br>Project Management Services<br><br>***Ratings to be awarded as follows:***<br>1. **Score 1=** *No Implementation Road map/ Project Plan provided*<br>2. **Score 2=** *Insufficient implementation Road map with no design and no maintenance plan*<br>3. **Score 3=** *Detailed Implementation Road map/project plan with design, project management plan and rollout plan*<br>4. **Score 4=** *Detailed Implementation Road map with design, project management plan and rollout plan, detailed maintenance and support plan Detailed*<br>**5. Score 5=** *detailed Implementation Road map/project plan with best practises in designs, detailed project management plan and detailed rollout plan with timeframes and detailed maintenance and support plus tools and techniques to be used*<br>**NB: The Project plan must entail ALL requirements.** | | | | | | **25** |

| No | EVALUATION CRITERIA | Rating | | | | | Weight |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | |
| 4. | **Technical Certification:**<br>The bidders must attach OEM Technical Certification for the proposed solution – Minimum 2 technical certification<br>**Technical Certification:**<br>The bidders must attach a minimum of 2 CVs of resources to be involved in the project plus, OEM Technical Certification for the Technical Resources.<br>***Ratings to be awarded as follows:***<br>1. ***Score 1*** = *Attached CV's +No Security Certification*<br>2. ***Score 2*** = *Attached CV's + only one Security Certification*<br>3. ***Score 3*** =*Attached CV's + two Security Certification*<br>4. ***Score 4*** =*Attached CV's + three Security Certification*<br>5. ***Score 5*** = *Attached CV's + 4 Advanced Security Certification (CISSP, CISM, CEH, CCSP, etc.)*<br>**Certifications must be relevant to the proposed solutions.** | | | | | | 25 |
| 5. | **Reference Checks**<br>A minimum of two (**2**) contactable references where you have delivered a Security Operations Centre service in the last 3 years to a minimum of 500 seats each.<br>***Ratings to be awarded as follows:***<br>1. ***Score 1*** – *No reference letters of completed projects.*<br>2. ***Score 2*** – *Only one reference letters of completed projects.*<br>3. ***Score 3*** – *Two reference letters of completed projects.*<br>4. ***Score 4*** – *Three to Five reference letters of completed projects.*<br>5. ***Score 5*** – *Six to Ten reference letters of completed projects*<br>**References must be South African and not international; they must be properly dated.** | | | | | | 20 |
| | **TOTAL** | | | | | | 100 |

1. Functionality will count out of 100 points. Bidders must achieve a minimum score of ***60 points out of 100*** on the functionality evaluation to proceed to the next phase.

2. **Bidders that achieve less than 60 points on functionality will be disqualified for further evaluation.**

**Please Note:** CIPC 6.1 Preference Points Claim Form in terms of the PPPFA is attached for claiming above mentioned points, if not completed the company will automatically score 0 points.

**Preferential Procurement Policy**

The bidders that have successfully progressed will be evaluated in accordance with the 80/20 preference point system contemplated in the Preferential Procurement Policy Framework Act (Act 5 of 2000).

**Pricing**

Pricing will be calculated using the lowest price quoted as the baseline, thus the lowest price quoted will achieve full marks, while all other quotes will achieve a weighted average mark based on the lowest price.

| Description | Total |
|---|---|
| Price | **80** |
| BBBEE | **20** |
| **Total** | **100** |

**The bidder with the highest score on price will be recommended as the successful service provider.**

Companies and Intellectual

# 20. ANNEXURE A: PRICING SCHEDULE –

**(THE PAGE MUST BE INCLUDED IN THE PRICE FOLDER USB AS WELL AS PRICE ENVELOP)**

Prospective bidders **must submit a bill of quantities clearly** indicating the unit costs and any other costs applicable. The onus is upon the prospective bidders to take into account all costs for the duration of the contract period and to CLEARLY indicate the price.

***BID COSTING***

**PRICING TABLE (TO BE COMPLETED; PRINTED AND INCLUDED IN THE SEALED ENVELOP -PRICE PROPOSAL) WITH THE FOLLOWING DOCUMENTS**

1. **SDB 3.3: PRICING SCHEDULE**
2. **SBD FORM 1: INVITATION TO BIDS**
3. **A BIDDER *MUST* ATTACH *PRICE BREAKDOWN IN THE BIDDER'S COMPANY LETTERHEAD STATING UNIT COSTS AS WELL AS THE TOTAL BID PRICE INCLUSIVE OF ALL FOR THE DURATION OF THE CONTRACT***
4. **BIDDER'S TO COMPLY WITH ALL CONDITIONS BELOW AS WELL AS THOSE ON PAGE 6 OF 18 AND PAGE WITH REGARDS TO PRICE**

**The costing should be based on all requirements of the terms of reference for a period 5 YEARS costs applicable**. The onus is upon the prospective bidders to take into account all costs and to CLEARLY indicate the price. Cost breakdown must be provided, covering all required aspects in this tender. **NB The total price must be carried over to the pricing schedule and *will be used to evaluate the bids*. Prices must be firm for the duration of the project. PRICE CARRIED OVER TO SBD FORM 3.3 AND SBD FORM 1 MUST INCLUDE ALL COSTS FOR THE DURATION OF ALL PERIOD STATED ABOVE UNDER PRICING. *FAILURE TO COMPLY WITH THIS REQUIREMENT SHALL IMMEDIATELY INVALIDATE THE BID.***

**TABLE 1: (FORMAT FOR PRICE QUOTATION):**

***TERM: 5 YEARS***

| Phase/ Stage | High level Activities | Time Frames | Deliverable(s) | Comments (if any) | Budget (incl. VAT) |
|---|---|---|---|---|---|
| *e.g. Stage 1* | | *Measured in weeks/ days* | | | |
| | | ***TOTAL DURATIONS:*** | | | |

The suppliers must break down payment as per deliverable on the project plan. Reports are to be developed and presented per deliverable, e.g.

| No. | Deliverable | Quantity | R |
|---|---|---|---|
| 1 | Hardware and Software Installation | As proposed | |
| 2 | HA Configuration | As proposed | |
| 3 | Other Security Features | As proposed | |
| 4 | Event Logging and Reporting | As proposed | |
| 5 | Other Components | As proposed | |
| 6 | Professional Support<br>(Please show per component) | As proposed | |
| 7 | Implementation<br>(Please show per component) | As proposed | |
| 8 | Additional Project/Support Hours | 7400 hours | |
| | Total | | |

| Year 1<br>(R000) | Year 2<br>(R000) | Year 3<br>(R000) | Year 4<br>(R000) | Year 5<br>(R000) | Total<br>(R000) |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| TOTAL FOR PERIOD OF 5 YEARS | | | | Price VAT excl. | |
| | | | | VAT | |
| | | | | TOTAL | |

The suppliers must break down payment as per deliverable on the project plan. Reports are to be developed and presented per deliverable, e.g.

**Note: Service providers will be responsible for all costs e.g. transportation for ALL activities associated with this bid.**

**TOTAL PRICE TO BE STATED BELOW FOR THE TENDER FOR THE DURATION OF THE CONTRACT TO BE CARRIED OVER TO SBD3.3 AND FORM 1**

| | VAT amount | Amount Inclusive of VAT (Incl. of ALL) |
|---|---|---|
| **TOTAL FOR A PERIOD OF 5 YEARS**<br>**(Ceiling price to be carried over to SBD 3.3 and form 1 for the duration of the contract. the total bid price will be used for price evaluation purposes)** | | |

**Note: Service providers will be responsible for all costs e.g. transportation for ALL activities associated with this bid.**

- Provide fixed price quotation for the duration of the contract
- **Cost must be VAT inclusive and quoted in South African Rand**
- Costing should be aligned with the project activities / project phases

***FAILURE TO COMPLY WITH ALL THE ABOVE REQUIREMENTS FOR PRICING SHALL IMMEDIATELY INVALIDATE THE BID.***

## 21. BRIEFING SESSION

**PLEASE NOTE THAT THERE IS NO BRIEFING SESSION SCHEDULED FOR THIS.**

| | |
|---|---|
| ***COMPULSORY*** **BRIEFING SESSION/SITE VISIT** | **NONE** |

## 22. SUBMISSION OF PROPOSALS

Sealed proposals will be received at the Tender Box. **THE CIPC TENDER BOX HAS THE FOLLOWING DESCRIPTION: "CIPC**

**THE BID BOX IS SITUATED AT: AT THE WEST GATE ON 77 MEINTJIES STREET, CLOSE TO ENTFUTFUKWENI BUILDING (BLOCK "F"), 77 MEINTJIES STREET, SUNNYSIDE, "THE DTI" CAMPUS, PRETORIA.**

**Proposals must be addressed to:**

Manager (Supply Chain Management)
Companies and Intellectual Property Commission (CIPC)
Block F, **the DTIC** Campus, 77 Meintjies Street,
Sunnyside
PRETORIA

**ENQUIRIES**

**A. Supply Chain Enquiries**

Ms Ntombi Maqhula OR Mr Solomon Motshweni
Contact No: (012) 394 3971 /45344
E-mail: Nmaqhula@cipc.co.za OR **SMotshweni@cipc.co.za**

**B. Technical Enquiries**

**Mr. Sphiwe Mbatha E-mail : smbatha@cipc.co.za**
**OR**
**Mr. Andile Stulo E-mail : astulo@cipc.co.za**
**OR**
**Mr Solly Bopape E-mail: sbopape@cipc.co.za**

***Note : It is the bidder's responsibility to call CIPC if they have any questions that have not been answered via email, as the system may have flagged their email as spam.***

## 23. DEADLINE FOR SUBMISSION

**BIDS OPENING DATE:** **29 JULY 2023**

**BIDS CLOSING TIME:** **11: 00 AM**

**BIDS CLOSING DATE:** **19 JULY 2023**

***BIDDERS MUST ENSURE THAT BIDS ARE DELIVERED IN TIME TO THE CORRECT ADDRESS. LATE PROPOSALS WILL NOT BE ACCEPTED FOR CONSIDERATION***

**NB:** ***IT IS THE PROSPECTIVE BIDDERS' RESPONSIBILITY TO OBTAIN BID DOCUMENTS IN TIME SO AS TO ENSURE THAT RESPONSES REACH CIPC, TIMEOUSLY. CIPC SHALL NOT BE HELD RESPONSIBLE FOR DELAYS IN THE POSTAL SERVICES AND BID DEPOSITED IN THE INCORRECT BID BOX.***