Companies and Intellectual
Property Commission

a member of the dti group

# ANNEXURE "H"

# TERMS OF REFERENCE ("TOR")

| | |
|---|---|
| **CIPC BID NUMBER:** | **06/2023/2024** |
| **DESCRIPTION:** | **INVITATION TO ICT SERVICES PROVIDERS TO PROVIDE A NEXT GENERATION FIREWALL SOLUTION (NGFW)** |
| **CONTRACT PERIOD:** | **THREE (3) YEARS.** |
| **BID CLOSING DATE:** | **12 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".**

**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) Bidders 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 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 PAGE 20***

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 17 AND 20-** REQUIREMENTS ON PRICE PROPOSAL **AND ANNEXURE "A"**

**NB: Bidders must also refer to page 17 of 22 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.***

## 4. PURPOSE

To procure the supply, implementation and support of a Next Generation Firewall solution. The current two internal NGFW Fortigate 3240C are on EOL hence this procurement is required to maintain internal security of CIPC. Two of the external facing firewall FG 2000E licensing is expiring December 2022 need replacement. In essence both the internal and external firewalls need to be renewed.

## 5. BACKGROUND

In compliance with the Companies Act 2008, CIPC must provide the following services:

- Registration of corporate entities and intellectual property rights;
- Maintenance of accurate, up-to-date and relevant information concerning companies, corporate entities and intellectual property rights, and the provision of that information to the public and to other organs of state;
- The promotion of education and awareness of company and intellectual property laws, and related matters;
- The promotion of compliance with the Companies Act, and any other applicable legislation;
- Widest possible enforcement of the Companies Act;
- Promotion of the reliability of financial statements by monitoring compliance;
- Promoting voluntary resolution of disputes arising in terms of the Companies Act; and
- Research and reporting on matters of national policy and intellectual property law.

## 6. REQUIREMENT

CIPC has adopted a multi-layered, defense-in-depth security strategy to minimize the possibility of various threats being exploited and to optimize our investment in security solutions. As part of our network layer security strategy, we wish to implement various layers of next generation firewall.

**CIPC WANTS TO ACQUIRE NEXT GENERATION FIREWALL SOLUTION WITH AT LEAST THE FOLLOWING CAPABILITIES:**

| Solution | Description |
|---|---|
| **Technical Requirements** | NGFW Capabilities All security subscriptions enabled (Threat Prevention, IPS, URL, DNS Security, and Zero Day) - Identify applications, not ports. Identify exactly what the application is, across all ports, irrespective of protocol, encryption (SSL or SSH), or evasive tactic. The application identity becomes the basis for all security policies. - Identify users, not IP addresses. Employ user and group information from enterprise directories for visibility, policy creation, reporting, and forensic investigation—no matter where the user is located. |
| **Network Capabilities** | • Protection and Detection of device ID as well as URL Filtering device.<br>• The solution should allow for BYOD security including sandboxing and document encryption<br>• The NGFW must be flexible for deployment at L2 and L3 modes for VLANs. It must support dynamic routing capabilities, e.g. OSPF, BGP & RIP, including full 802.1q VLAN and support for virtual wire.<br>• The NGFW must provide a graphical view of real-time bandwidth monitoring for; session consumption at the application and user level within the selected QoS class.<br>• The NGFW must allow for the interfaces to be mapped at the security zones for defined security policy purposes.<br>• The NGFW must provide full application visibility, control, inspection, monitoring and logging for applications using IPv6.<br>• The NGFW must use the application, not the port, as the basis for all policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.<br>• The NGFW must support QoS marking and reclassification based on source/destination IP, port, protocol, and application<br>• The NGFW solution must provide support for access control for predefined services, protocols and connections.<br>• The NGFW must easily integrate firewall policies with 802.1X wired, wireless, proxies, network access control, and any other source of user identity information.<br>• The NGFW must inspect all traffic to automatically block known vulnerabilities, malware, vulnerability exploits, spyware, command and control (C2), and custom intrusion prevention system (IPS) signatures. |

| | |
|---|---|
| | • The NGFW must protect against unknown file-based threats, automatically delivering protections in real time or less for most new threats across networks, endpoints, and clouds<br>• The NGFW must deliver the same throughput and performance with application control active.<br>• The NGFW must be able to manage encrypted and authenticated traffic with PKI Certificates.<br>• The solution must support HTTP, HTTPS proxy, DHCP as well as transparent or bridge mode.<br>• All required performance specifications shall be from published public sources (not white papers) from production environments with all required features and applications simultaneously active.<br>• To prevent evasive users and applications from bypassing security functions, all product functions for IPS, Threat Prevention, and Anti-Virus, shall not require specific software port and protocol combinations for detection, mitigation, or enforcement.<br>• The NGFW should include a Zero -Day threat prevention system that validates executable files and urls passing through the firewall and provides automatic cloud-based behavioral threat analysis of unknown executables, and automatic signature creation to block delivery for executable files that are deemed dangerous by the analysis system.<br>• The NGFW must have the ability to work with Standards based protocols;<br>• VoIP Compliant (Avaya)<br>• H323 Compliant<br>• H225 Compliant<br>• Support for AAA protocol<br>• Multi-cast Compliant<br>• IPv4 and IPv6 compliant<br>• Provide High Availability |
| **Application Control** | • The NGFW must use the application, not the port, as the basis for all policy decisions: allow, deny, schedule, inspect, and apply traffic-shaping.<br>• The firewall application control policy must use application usage control policies that can be enforced using a combination of the following parameters:<br>○ Allow or deny<br>○ Allow but scan<br>○ Allow based on schedule<br>○ Decrypt and inspect<br>○ Apply traffic shaping<br>○ Allow for certain users or groups<br>○ Allow certain application functions<br>○ Any combination<br>• The NGFW's enforcement model policy must have the ability for blocking bad applications, protecting the business applications and promoting the secure use of end-user applications.<br>• The NGFW must categorize unidentified applications for policy control, threat forensics, or App-ID technology development.<br>• The NGFW must support the ability to enforce Multi-Factor Authentication to internal applications<br>• The NGFW must provide full visibility into the details of all TLS-encrypted connections and stop threats hidden in encrypted traffic, including traffic that uses TLS 1.3 and HTTP/2 protocols.<br>• The NGFW shall process all data for all active services as a single stream to minimize delay and jitter in order to ensure optimal performance for delay and jitter-sensitive applications, such as VOIP, High Definition video, and future real-time sensitive applications<br>• The NGFW shall be able to identify the application, regardless of port, SSL/SSH encryption, or evasive technique employed, to prevent evasive tactics used by modern hackers and malware<br>• The NGFW must seamlessly integrate with Microsoft Active Directory / Azure Active Directory.<br>• The NGFW must have the ability to create granular security policy definitions per user and groups to identify, block or limit usage of web applications and widgets like instant messaging, social networking, video streaming, VoIP, games and more.<br>• The NGFW must provide application function control to identify, allow, block or limit usage of applications and features within them.<br>• The NGFW must detect and block known and unknown threats over DNS while predictive analytics disrupt attacks using DNS for C2 or data theft.<br>• The NGFW must prevent access to malicious sites and protects users against web-based threats.<br>• The NGFW must enable safe internet use while protecting against threats and malware. Scan for viruses and malware in allowed collaborative applications. Should have ability to<br>○ protect environments with social media and internet applications. |

| | |
|---|---|
| | • The NGFW must have the ability to create detailed policies that are based on characteristics such as user identity, user role and specific aspects of a web application. This must be advanced user and application controls such as ability to expand user groups, domain names as well as detailed user and application usage information in reports, logs and statistics. To reduce administrative costs, overhead, and human error, the NGFW shall simplify management by having a single tab for configuring policy for all running features, including application, user, and content id's. It shall be able to use all three identification methods in a single policy, to accept or deny traffic, packet shape, QOS, and Policy route traffic. |
| **Threat Prevention** | • The solution's threat prevention mechanism must update worldwide and have the ability to handle zero-day attacks across all next generation threat prevention applications including IPS, Application Control, URL filtering, DNS Security, DLP, IOT, and Anti-virus.<br>• The NGFW must have built in IOT control on the NGFW along with device context in a policy.<br>• The NGFW must be able to provide Machine Learning algorithms for advanced protections directly from the NGFW with no external connections needed.<br>• The NGFW must support the ability to identify Domain Generating Algorithms to protect against data exfiltration<br>• The NGFW must have direct enforcement, C2 prevention and Vulnerability management and protection.<br>• The bidder must provide detailed information for re-categorization of URL, in the event of a compromised website and possible distribution of malware.<br>• The advanced malware analysis (malware sandboxing) solution must have MacOS and Linux executable scanning by default.<br>• The NGFW must support credential theft and allows for;<br>o Blocks known bad phishing sites<br>o Blocks user logins attempts from suspicious regions<br>o Blocks credential reuse for non-corporate assets<br>o Inserts Multi-Factor Authentication mid-stream when anomalous activity detected<br>• The NGFW must specify the type of incident management including accelerated forensics or incident investigation with a centralized, correlated view across all of the logs for traffic, threats, URLs, and applications related to an individual session.<br>• The solution must provide the ability to Increase security with automatic sharing of new attack information with other gateways in means of signature updates etc.<br>• The NGFW must be able to intercept, decrypt and re-encrypt SSL/TLS, SSH, and VPN traffic with low performance degradation.<br>• The NGFW must be able to decrypt incoming and outbound SSL traffic.<br>• The NGFW must have intrusion prevention features that can block both known and unknown network and application layer vulnerability exploits.<br>• protect against a wide range of malware including viruses, (both HTML and JavaScript), Spyware, Trojans, and have an inline AV and ML protection engine that can detect and block viruses by scanning and inspecting traffic, and the ability to send files in real time to a sandbox, protect against zero-day attacks before static signature protections have been created providing integrated malware protection.<br>• The NGFW must have an integrated Botnet and Anti-Virus application support to detect and stop and report abnormal network traffic behavior. The NGFW must have a central Botnet event correlation and reporting console to monitor scanned bots' actions.<br>• Integrate with the cloud based sandboxing platform for detection of Zero Day attacks and deploy consistent policies to local and remote users running on Windows,<br>o MacOS, Linux, Android, or Apple iOS platforms |
| **VPN and Remote Access** | • The required Standards-based site-to-site IPSec VPN connectivity must be combined with application visibility and control enabled protected communications between two or more devices or another vendor's IPSec VPN device.<br>• SSL VPN must provide secure network access for remote users and extend policy-based visibility and control over applications, users and content to those users.<br>• The SSL VPN must achieve the highest security of data streams to achieve confidentiality.<br>• The NGFW must provide SSL VPN Client for protecting users and corporate assets when users roam off of the protected corporate network.<br>• The NGFW must be able to acquire User Identities from: LDAP, Captive Portal, VPN, NACs (XML or API), Syslog, Terminal Services, XFF Headers, Server Monitoring, AND client probing |

**FAILURE TO COMPLY WITH THIS REQUIREMENTS SHALL IMMEDIATELY DISQUALIFY A BIDDER.**

| SOLUTION CAPABILITIES | COMPLY / NOT COMPLY (Include Document/Page #) |
|---|---|
| Assess the security and health of your network and the impact of your future deployment options with proactive insights and gain confidence in your network stability. | |
| Automatically detect security gaps in your network and become proactive with ML-powered anomaly detection, and actionable insights into the health and performance of the entire deployment | |
| Provides a comprehensive view of threats across firewalls, security subscriptions, and network traffic. | |
| Analytics for operational health: Uses ML-driven techniques for predictive insights and performs root cause analysis. | |
| Provides best practices and policy recommendations customers to customer's unique environment to improve security posture. | |
| Stops all known threats on the market-leading NGFW without sacrificing performance.<br>Gartner data sheet or other verifiable proof should be provided | |
| Deploy rapid coverage for emerging and custom threats with automated IPS workflows supporting Snort and Suricata. | |
| Stop zero-day injection attacks inline. | |
| Prevent all known threats as they are discovered, inspect real traffic for new & unknowns | |
| Stop 0-day exploits, evasive C2 attacks inline and reduce business risk, costs on post-execution investigation | |
| Solution needs to provide Patented Deep Learning Models - please elaborate how your solution works from a deep learning point of view | |
| Solution needs to provide Injection Attack Detector capabilities - please elaborate how your solution works from an injection attack detector point of view | |
| Solution needs to cater for SSL Decryption and Encryption on the same appliance | |
| Prevent evasive C2 traffic over web and non-web protocols including those derived from hacking tools such as Cobalt Strike - please explain how your solution work | |
| The solution needs to ensure malware analysis that is capable of preventing the most evasive threats with unmatched speed and scale - please explain how your solution work | |
| Ability to prevent highly evasive malware | |
| Solution should include Intelligent Run-time Memory Analysis - please explain | |

| | |
|---|---|
| Solution needs to do Automated Unpacking and Stealthy Observation - please explain | |
| Solution needs to cater for Malware Family Fingerprinting - please explain | |
| Solution needs to reduce actionable events and workload for the SOC - please explain | |
| Solution needs to determine if never-before-seen file is malicious or not - please explain | |
| Solution should ensure low false positive rate - please explain | |
| Solution should proactively prevent weaponized files, credential phishing and malicious scripts without compromising business productivity - please explain | |
| Solution should  inspects files at line speed and needs to block malware variants of portable executables as well as Powershell files - please explain | |
| Solution should identify phishing pages and malicious JavaScript in milliseconds, stopping them inline so nobody in your network ever sees them. - please explain | |
| Solution needs to automatically prevent all known threats across all traffic in a single pass - please explain | |
| Extend Security capabilities to your remote users to provide consistent security everywhere in your environment. - please explain | |
| Solution should use inline machine learning, identify and disrupt the latest attacks that abuse DNS. - please explain | |
| Solution should have a single coordinated network security stack for all alerts, policies, rule violations, IDPS, web security, malware analysis and DNS - please explain | |
| Solution should have Unparalleled protection from DNS-based threats through and inline ML algorithms that predict and identify new and advanced threats, disrupting attacks. - explain | |
| Solution should assist to detect exploitative DDNS services by filtering and cross-referencing DNS data from various sources to generate candidate lists, which are then further validated to maximize accuracy. - please explain | |
| Solution should be able to Discover Newly registered domains - please explain | |
| Solution needs to discover Park domains and protect users against this - please explain | |
| Solution needs to protect against Proxy avoidance and anonymizers - please explain | |
| Solution should protect against DNS Sinkholing - please explain | |
| Solution should identify Domain Generation Algorithm - please explain | |
| Solution should protect against Fast Flux Domains - please explain | |
| Solution should enables threat inspection and the decision to enforce forward/no forward to be done in a single policy. - please explain | |
| Solution should be able to map the IP addresses to (e.g., Active Directory) users and users to groups (roles) to enable visibility and policy enforcement by user and group. - please explain | |
| Solution should identify applications with a combination of application signatures, protocol detection and decryption, protocol decoding, and heuristics. - please explain | |

| | |
|---|---|
| Solution should use an uniform signature format to scan traffic for threats (exploits, viruses, spyware and malware communications) and sensitive data patterns (e.g., ID Numbers and credit card numbers etc.) - please explain | |
| Solution should cater for write single policies for Malware prevention, URL Filtering, IPS etc. - please explain | |
| Solution should allow for visibility into All ports, protocols and applications used by users - please explain | |
| Solution should use stream based engine - please explain | |
| Solution should provide actionable insights regarding firewall health and predict firewall disruptions with recommendations. | |
| NGFW traffic logs, proactively identify and remediate inefficiencies in security policies | |
| NGFW should include web proxy bundled in a solution | |
| **Mandatory System Requirements (2 X HA External/Perimeter Firewalls)**<br>• Interfaces such as 1G/2.5G/5G/10G (12), 1G/10G SFP/SFP+ (10), 25G SFP28 (4)<br>• Management interfaces 100/1000 out-of-band management port (1)<br>• 100/1000 high availability (2), 10G SFP+ high availability (1)<br>• RJ-45 console port (1), Micro USB (1)<br>• 480 GB SSD Storage capacity<br>• Redundant power supplies<br>• Support at least 10Gbps of firewall throughput for HTTP and application mix transactions.<br>• Support for a minimum of 6Gbps of IPsec VPN throughput.<br>• Support for a minimum of 1 000 000 sessions<br>• Support for 2.5Gbps and 5Gbps Ethernet ports.<br>• The proposed hardware firewall model must ensure throughput of 4.7 Gbps after ALL security features are enabled i.e IPS, NGFW, Threat Prevention, AntiMalware. | |
| **Mandatory System Requirements (2 X HA Internal Firewalls)**<br>• 1G/2.5G/5G/10G (8), 1G/10G SFP/SFP+ (12), 25G SFP28 (4), 40G/100G QSFP+/QSFP28 (4)<br>• Management interfaces<br>• 1G SFP out-of-band management port (1),<br>• 1G SFP high availability (2), 40G QSFP+ high availability (1),<br>• RJ-45 console port (1), Micro USB<br>• 480 GB SSD pair, system storage capacity<br>• Redundant power supplies<br>• Support at least 38Gbps of firewall throughput for HTTP and appmix transactions. | |

| | |
|---|---|
| • Support for a minimum of 20Gbps of IPsec VPN throughput.<br>• Support for a minimum of 3 000 000 sessions<br>• Support for 2.5Gbps and 5Gbps Ethernet ports.<br>• The proposed hardware firewall model must ensure throughput of 40Gbps after ALL security features are enabled i.e IPS, NGFW, Threat Prevention, AntiMalware. | |
| **Operating System & Mgmt. Access**<br>• Should support both a management plane and a data plane with visibility in a dashboard to clearly understand usage and metrics.<br>• The NGFW must support protocols for management traffic such as;<br>• Ping,Telnet, HTTP,HTTP OCSP, HTTPS and snmp.<br>• The NGFW should have services that permits for management traffic;<br>• Response pages, Captive Portal, URL Admin Override, User-ID, | |
| **Visibility & Monitoring and Reporting**<br>The proposed system shall provide robust visibility GUI panels and dashboards that show network activity, threat activity, blocked activity, tunnel activity, SSL activity.<br>• Reporting to be bundled in the solution | |
| **High Availability**<br>• The NGFW must support the following;<br>• Active Passive and Active Active<br>• The NGFW must support HA Links and Backup Links including;<br>• Control Link, Datalink along with additional back up links. | |
| **Load Balancer (2 X Load balancer HA)**<br>• Integrated Application Protection<br>• Comprehensive application protection via embedded WAF, bot management, threat intelligence and API protection capabilities to ensure application availability.<br>• Single, comprehensive solution to manage application traffic, ensure continuous service in and across cloud and data centre locations and secure your applications, APIs and data.<br>• Next-generation application delivery controller (ADC) needs to deliver on applications SLA.<br>• Real time visibility and actionable insights for proactive management of application availability and security issues.<br>• Simplify application delivery planning and deployment via a single global elastic license that enables ADC services to be allocated across any environment.<br>**Required Performance (WAF)** | |

| | |
|---|---|
| • Total Max. Throughput: 24 – 80 Gbps scalable<br>• Max. CPS (new connections per second): 450K to 1.39M CPS<br>• Max. CEC (concurrent connections): 4 – 12 Million Scalable<br>• Max. SSL Throughput: 4.8 – 7.7 Gbps<br>• Max. SSL CPS/TPS:4000<br>• Max. RPS (in case of WAF): 850k RPS TO 3M RPS<br>• Amount of Dynamin HTTP/s calls in a month:It depend on-boarding of new apps – currently | |
| • Must be in the leaders Magic quadrant 2023 | |

| Capability | Description |
|---|---|
| **Knowledge & Expertise** | The supplier must demonstrate and provide evidence of knowledge and experience in implementing similar solution and understanding of CIPC or similar business environments. |
| **Resources** | The supplier must have sufficient quantity and quality of resources with appropriate skill and/or certification to implement and support the solution provided. |
| **Project Management** | The supplier must use sound project management approaches to ensure success of development, implementation and support projects. |
| **Support** | The supplier must be able to meet agree service levels, use effective processes, standards and procedures for service management and must be able to call on the solution vendor/manufacturer for support if required. |
| **Training & skills transfer** | The supplier must be able to provide training for and transfer knowledge to CIPC staff training to effectively manage and support the solution. |

**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.

## 7. SCOPE OF WORK

Provide a Next Generation Firewall solution consisting of:

- 4 hardware appliances (**Internal** 2 X HA and **External** 2 X HA NG firewalls)
- Network Intrusion Prevention with Machine Learning included in solution;
- Advanced Web Filtering with Machine learning included in solution;
- 2 X Load balancing Web Application Firewall Appliances
- NGFW security event logging and reporting solution;
- Implementation of the solution;
- Support and maintain for the solution for 3 Years;
- Define and/update processes, policies, standards and procedures for network security and firewall management;
- Provide ad hoc project or other services as required; and
- Train and transfer skills to CIPC staff.

## 8. TIME FRAMES

The service providers should indicate through a project plan how they will design, implement and support the solution over a **3 Years' period.**

## 9. COSTING

- **Please refer to Annexure A for the details 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.

## 10. REPORTING

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

### 10. WORKING CONDITIONS

### 10.1 Equipment

N/A

### 10.2 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.

### 10.3 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.

### 10.4 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 requirement.

- The resource must at all times follow the security measures and obey the rules as set by the organization.

**10.5 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.

## 11. 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.

## 12. 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).

### 12.1 Evaluation (Phases)

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

Phase 1: Compliance to minimum requirements

Phase 2: Functional Evaluation

Phase 3: 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. The bidder(s) proposal *may* be disqualified for non-submission of any of the documents. **Bidders shall submit a letter from the OEM Certification/Partner:**

| 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>**Compliance to ANNEXURE A: PAGE 16 AND 17**<br>**REFER TO PAGE 5 TO 6 and 18**<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>**REFER TO PAGE 5 OF 20** | | 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 from the OEM Certification/Partner: ***The letter must be** for each of the three solutions as per the TOR*<br>- The bidders must provide a letter from Solution Vendor which indicates that they are accredited to implement, supply and support the proposed solution<br>- In the event that the bidder is the owner of the proposed Product/Solution/Systems/Technology, a letter must be attached for confirmation.<br>**FAILURE TO SUBMIT WILL RENDER YOUR BID BEING DISQUALIFIED** | | - **The letter or a testimonial must be submitted in order to proceed to the next phase** (phase 2). Bidders to ensure that a letter/ testimonial /certification etc. addressing this requirement is attached.<br>- All bidders are required to comply with this requirement.<br>- **Should there be no letter/ testimonial /certification etc attached for each solution the bid *will immediately be disqualified.***<br>- The letter/ testimonial /certification must be signed dated by authorized representative<br>- It should state expiry date or validity<br>**FAILURE TO SUBMIT WILL RENDER YOUR BID BEING DISQUALIFIED** |

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

## PHASE 2: 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>• Demonstrate how the proposed solution will be implemented.<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>***Ratings to be awarded as follows:***<br>***1=** Not comply with solution capabilities.*<br>***2=** Partly addressed solution capabilities.*<br>***3=** Designs and Architect a solution as per OEM best practices, comply with all solution capabilities requirements.*<br>***4=** Meet No 3 above requirements plus training and certification, knowledge and skills transfer plan and Integration with CIPC's entire Environment.*<br>***5=** Meet No 4 requirements plus , 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 .* | | | | | | **40** |
| 2 | **Accreditation with Original Equipment Manufacturer (OEM)**<br>• **The bidders must attach their Partner Certification**<br>• The bidders must provide a letter from OEM, which indicates that they are accredited to implement, supply and support the proposed solution.<br>***Ratings to be awarded as follows:***<br>***1=**No partner certification*<br>***2=** Partner Certification*<br>***3=** Partner Certification and accreditation OEM Letter*<br>***4=** Partner Certification and accreditation OEM Letter for implementation of NGFW*<br>***5=** Partner and accreditation OEM Letter for implementation of NGFW and AFW/Load balancer* | | | | | | **10** |
| 3 | Project Plan<br>Methodology and Approach on how the bidder will achieve the following .<br>NGFW implementation and rollout plan<br>WAF implementation and rollout plan<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 | | | | | | **10** |

## PHASE 2: FUNCTIONAL EVALUATION AND COMPLIANCE TO SPECIFICATION

| No | EVALUATION CRITERIA | Rating | | | | | Weight |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | |
| 4 | **Competency Requirements**<br>• The bidders must meet these requirements<br>• Company Record for NGFW projects.<br>• 4 years experience provisioning of NGFW Solution(The experience measured herein below is the number of cumulative years of the company in delivering NGFW projects).<br>***Ratings to be awarded as follows:***<br>**1=***Experience less than or equal to 3 years*<br>**2=***Experience greater than 3 years, but not more than 4 years*<br>**3=***Experience greater than 4 years, but not more than 5 years*<br>**4=***Experience greater than 5 years, but not more than 6 Years*<br>**5=***Experience greater than 6 Years*<br>**Proof to be submitted: testimonial letters from clients** | | | | | | **25** |
| 5 | **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 for both NGFW proposed and WAF<br>***Ratings to be awarded as follows:***<br>**1=***Attached 2one CV with NGFW Certification*<br>**2=***Attached 2 CV's with oNGFW Certification*<br>**3=***Attached 2 CV's + NGFW; and one Advanced Security certification (CISSP, CISM, CEH, etc)*<br>**4=***Attached 2 CV's + NGFW; and Advanced Security Certification + 1 additional Security Reporting Certification*<br>**5=***Attached CV's + NGFW; and Advanced Security Certification + 2 more Security Reporting Certification* | | | | | | **15** |
| | **Total** | | | | | | **100** |

**Note:**

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 will be recommended as the successful service provider.**

## 13 ANNEXURE A: COSTING

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 Three (3) years . Pricing to be presented as per the tables below.**

Prospective bidders **must submit a total price as per table below clearly indicating the unit costs and any other 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):

The supplier must provide a comprehensive project plan supported by a project schedule as recommended below:

| 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:*** | | | | | |
| ***TOTAL BUDGET (Incl VAT):*** | | | | | |

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

| No. | Deliverable | Quantity | R |
|---|---|---|---|
| 1 | Hardware and Software Installation NGFW | As proposed | |
| 2 | HA Configuration NGFW | As proposed | |
| 3 | Hardware and Software Installation WAF | As proposed | |
| 4 | HA Configuration WAF | As proposed | |
| 5 | Other Security Features | As proposed | |
| 6 | Event Logging and Reporting | As proposed | |
| 7 | Other Components | As proposed | |
| 8 | Professional Support ***(Please show per component)*** | As proposed | |
| 9 | Implementation ***(Please show per component)*** | As proposed | |
| 10 | Certified Classroom Technical Training for 3 Resources( both NGFW and WAF | As proposed | |
| 11 | Additional Project/Support Hours | 2400 hours | |
| | **Total** | | |

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

**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 |
|---|---|---|
| TOTAL<br>**(Ceiling price to be carried over to sbd3.3 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 COSTING SHALL IMMEDIATELY INVALIDATE THE BID.***

## 14 BRIEFING SESSION

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

| | |
|---|---|
| ***COMPULSORY***<br>**BRIEFING SESSION/SITE VISIT** | **NONE** |

## 15 SUBMISSION OF PROPOSALS

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

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

## 16 DEADLINE FOR SUBMISSION

| | |
|---|---|
| **BIDS OPENING DATE:** | **05 JULY 2023** |
| **BIDS CLOSING TIME:** | **11H00AM** |
| **BIDS CLOSING DATE:** | **12 JULY 2023** |

***BIDDERS SHOULD 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.***