



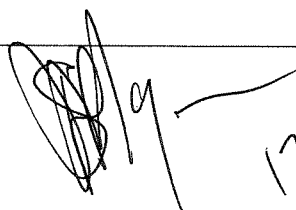
the doj & cd

Department:
Justice and Constitutional Development
REPUBLIC OF SOUTH AFRICA

REQUEST FOR BIDS

The Department of Justice and Constitutional Development invites all interested parties that are registered on SITA Contract RFB 1183/2014 to submit bids for requirements as stipulated below:

DOCUMENT NUMBER:	RFQ 07 2022
RFB ISSUE DATE:	17 October 2022
RFB CLOSING TIME AND DATE:	07 November 2022 @11:00 - Bids received after closing date and time will not be accepted <i>(Due to urgency of this service within the Department, there won't be any further extension on the closing date beyond the above, therefore prospective bidder (s) are advised to prepare their response in time and adhere to the closing date and time)</i>
RFB VALIDITY PERIOD:	120 Days (from RFB closing date).
DESCRIPTION:	APPOINTMENT OF A SERVICE PROVIDER FOR INFORMATION COMMUNICATION TECHNOLOGY (ICT) SECURITY SUPPORT SERVICES FOR A PERIOD OF 3 YEARS(INCLUSIVE OF ONE MONTH TRANSITIONING-IN AND ONE MONTH TRANSITIONING-OUT SERVICES WITHIN THE CONTRACT PERIOD)
PERIOD:	THREE (3) YEARS (INCLUSIVE OF ONE MONTH TRANSITIONING-IN AND ONE MONTH TRANSITIONING-OUT SERVICES WITHIN THE PERIOD).
BRIEFING SESSION TIME AND DATE:	NB: There will be NO Compulsory briefing session. Interested bidders are encouraged to send enquiries pertaining to this bid by e-mail to SCM@Justice.gov.za no later than 24 October 2022, quoting the bid number and description. Feedback on enquiries received will ONLY be published on Departmental website on 31 October 2022.
RESPONSES TO THIS RFB MUST BE FORWARDED TO:	Physical Address : Momentum Centre, 329 Pretorius Street, c/o Sisulu & Pretorius Street, Pretoria, 0001 Only Hand Delivery will be accepted and MUST be deposited/inserted inside the Tender Box which is situated at the Reception,
ENQUIRIES:	E-Mail all enquiries to SCM@justice.gov.za

 17/10/2022

Contents

SECTION 1	SCM PRE-QUALIFICATION	3
SECTION 2	EMPOWERMENT THROUGH SUBCONTRACTING.....	4
SECTION 3	MANDATORY REQUIREMENTS	7
SECTION 4	TECHNICAL SPECIFICATIONS	21
SECTION 5	TECHNICAL EVALUATION : FUNCTIONALITY PHASE.....	47
SECTION 6	PRICING SCHEDULES	57
SECTION 7	TERMS AND CONDITIONS FOR BIDDING.....	60
SECTION 8	GENERAL CONDITIONS OF CONTRACT (GCC).....	62
SECTION 9	BIDDING REQUIREMENTS AND SPECIAL BID CONDITIONS	63
SECTION 10	ANNEXURES	67
ANNEXURE A	OVERALL BIDDER EXPERIENCE.....	67
ANNEXURE B	BIDDER HUMAN RESOURCES EXPERIENCE	68
ANNEXURE B'	BIDDER HUMAN RESOURCES EXPERIENCE	69
ANNEXURE C	TRANSITION-IN / OUT REQUIREMENTS	72
ANNEXURE D	INVITATION TO BID SBD 1	80
ANNEXURE E	SBD 4.....	83
ANNEXURE F	SBD 6.1.....	85

SECTION 1 - SCM PRE-QUALIFICATION - DOCUMENTS THAT MUST BE FULLY COMPLETED AND SUBMITTED FOR SCM PRE-QUALIFICATION

DOCUMENT THAT MUST BE SUBMITTED	REQUIREMENT	NON-SUBMISSION WILL RESULT IN
		<u>DIS-QUALIFICATION</u>
BRIEFING SESSION	NO	A compulsory briefing session will not be held. All enquiries can be sent to SCM@justice.gov.za
INVITATION TO BID – SBD 1	YES	Complete and sign the supplied pro forma document
DECLARATION OF INTEREST – SBD 4	YES	Complete and sign the supplied pro forma document
PREFERENCE POINTS CLAIM FORM SBD 6.1	YES	Complete and sign the supplied pro forma document
TWO ENVELOPE SYSTEM	YES	In the “two envelope system”, prospective bidders are expected to package separate submissions in respect of the technical and financial proposals
GOOD STANDING ON TAX AFFAIRS	YES	The bidder must be in good standing with SARS in respect of any relevant legislative tax commitments and must provide together with the bid response a SARS pin number for verification purposes.
RADICAL ECONOMIC EMPOWERMENT	YES	<p>It is mandatory for all prime bidders to subcontract 30% of the value of the contract if their total bid price is above R 30 million. Proof of subcontracting arrangement between the main tenderer and the subcontractor must be submitted.</p> <p>Both the prime bidder and the sub-contractor must ensure that they comply with all the mandatory requirements and they must both be registered on CSD. Failure to comply with this requirement shall lead to disqualification.</p>

SECTION 2- EMPOWERMENT THROUGH SUBCONTRACTING

DETAILS OF THE NOMINATED SUB-CONTRACTOR / DEVELOPMENT PARTNER (if nominating more than 1 sub-contractor please duplicate this page)		
1	Name of Subcontractor	
2	Registration Number	
3	Vat registration Number	
4	Contact Person	
5	Telephone Number	
6	Fax Number	
7	Email address	
8	Postal Address	
9	Physical Address	
10	SARS pin number	
12	BBBEE level	

DECLARATION

I, the undersigned (name).....
certify that the information furnished above is correct. I confirm that I subscribe and I will accept to the conditions of "EMPOWERMENT THROUGH MANDATORY SUBCONTRACTING". I accept that the state may reject the bid or act against me should this declaration prove to be false.

Signature

Date

Position

Name of bidder

DOJ&CD NOTES ON THE EMPOWERMENT THROUGH MANDATORY SUBCONTRACTING

1. In terms of the PPPFA read together with the revised Preferential Procurement Regulations of 2017, the DoJ&CD is expected to fast-track the implementation of the regulation in order to achieve its small business empowerment objectives by encouraging skills transfer through meaningful sub-contracting or development partnership or incubator programs.
2. The bid response must demonstrate that the prime bidder has a programme or is willing to put a programme in place to incorporate small development partners (EME) or (QSE) registered on the CSD that are willing to meaningfully participate in the upstream or downstream services relating to core-services outlined in the RFB document.
3. The bidder may identify one or more sub-contractor / development partner using various empowerment models, including but not limited to provincial development partnerships, regional procurement strategies or centralized partnerships with decentralized operations in various provinces or regions, etc. The combination of any chosen sub-contracting model must be equivalent to a minimum of 30% of awarded contract value.
4. Prime bidder must be willing to provide reasonable access to the nominated sub-contractors / development partners to resources and the necessary training on various aspects of services to be delivered in terms of this RFB and be willing to implement a meaning technical skills transfer programme.
5. Prime bidder must be able to issue the necessary competency certificate to the nominated sub-contractor / development partner during the contract period.
6. The nominated subcontractor must be classified as EME or QSEs level enterprise of in terms of the new Preferential Procurement Regulations 2017 and must be registered on the CSD.
7. The DoJ&CD's (SCM) may make available the list of EME and QSEs registered on the CSD, however, it is the prerogative of the prime bidder to assess the subcontractor / development partner and identify areas of development, skills transfers and upstream / downstream participation and beneficiation in relevant maintenance and or support services relating to the core-services of the RFB. It is therefore advisable that potential

prime bidders independently identify subcontractor / development partner that have displayed interest in services outlined in the RFB.

8. The prime bidder must provide a memorandum of understanding or sub-contracting agreement as part of the bid response, demonstrating the intent to enter into a strategic sub-contracting arrangement or development partnership, subject to the award of this bid.
9. The prime bidder must provide supporting evidence as part of the bid response that the sub-contractor or development partner has confirmed willingness to participate in a strategic sub-contracting arrangement or development partnership, subject to the award of this RFB. This document may include the nature of services that may be negotiated post-award to form the basis for a strategic sub-contracting arrangement or development partnership.
10. As part of an effective Contract Management, the DoJ&CD may request the prime contractor to submit progress or status reports on the sub-contracting arrangement between itself and the sub-contractor or development partner.

SECTION 3 : MANDATORY REQUIREMENTS

1. MANDATORY REQUIREMENT

1.1 The submitted proposals will be evaluated by a panel on the basis of adherence/compliance to and submission of the following documentation and/or registration in terms of all relevant Legal institutions from each bidder or member of a consortium.

1.2 Bidders are required to **EXPLICITLY MARK "COMPLY** on each and every Mandatory requirement. Failure to do so will be taken as a **"DO NOT COMPLY"**.

Please note: If a bidder does not comply fully with each of the mandatory requirements, it shall be disqualified.

1.3 Where a requirement requires a bidder to provide substantiation / proof, the bidder shall provide such accordingly. If a bidder does not comply fully with each of the mandatory requirements, it shall be regarded as mandatory non-performance/non-compliance and the bid SHALL be disqualified.

1.4	ACCEPTANCE OF ALL CONDITIONS IN ALL THE SECTIONS OF THE RFB DOCUMENT	Comply																		
	The bidder confirms compliance with and acceptance of all the contents of this document and confirms that all sections of this document are contractually binding.																			
1.5	ACCREDITATION ON THE SITA TRANSVERSAL FRAMEWORK CONTRACT 1183/2014	Comply																		
	<p>Bidders should be accredited on the SITA 1183/2014 for the following services:</p> <p>A. ICT MANAGEMENT SERVICES</p> <table><tr><td>1. 81112011-0001</td><td>ICT Management – Technical Management</td></tr><tr><td>2. 81112011-0002</td><td>ICT Management - Functional Support Management</td></tr><tr><td>3. 81112011-0003</td><td>ICT Management - Contract Management</td></tr><tr><td>4. 81112011-0004</td><td>ICT Management - Program Management</td></tr><tr><td>5. 81112011-0005</td><td>ICT Management - Project Management</td></tr><tr><td>6. 81112011-0006</td><td>ICT Management - Project Administration Support</td></tr><tr><td>7. 81112011-0007</td><td>ICT Management - ICT Governance and Compliance</td></tr><tr><td>8. 81112011-0008</td><td>ICT Management - Document Configuration</td></tr><tr><td>9. 81112011-0009</td><td>ICT Management - Quality Management</td></tr></table>	1. 81112011-0001	ICT Management – Technical Management	2. 81112011-0002	ICT Management - Functional Support Management	3. 81112011-0003	ICT Management - Contract Management	4. 81112011-0004	ICT Management - Program Management	5. 81112011-0005	ICT Management - Project Management	6. 81112011-0006	ICT Management - Project Administration Support	7. 81112011-0007	ICT Management - ICT Governance and Compliance	8. 81112011-0008	ICT Management - Document Configuration	9. 81112011-0009	ICT Management - Quality Management	
1. 81112011-0001	ICT Management – Technical Management																			
2. 81112011-0002	ICT Management - Functional Support Management																			
3. 81112011-0003	ICT Management - Contract Management																			
4. 81112011-0004	ICT Management - Program Management																			
5. 81112011-0005	ICT Management - Project Management																			
6. 81112011-0006	ICT Management - Project Administration Support																			
7. 81112011-0007	ICT Management - ICT Governance and Compliance																			
8. 81112011-0008	ICT Management - Document Configuration																			
9. 81112011-0009	ICT Management - Quality Management																			

B. BUSINESS PLANNING AND DEVELOPMENT

1. 81112011-0010 Business Planning And Development - ICT Strategic Consulting
2. 81112011-0011 Business Planning And Development - Business Analysis
3. 81112011-0012 Business Planning And Development - Business Process Architecture
4. 81112011-0013 Business Planning And Development - Information Systems Architecture
5. 81112011-0014 Business Planning And Development - Information Architecture
6. 81112011-0015 Business Planning And Development - Information Technology Architecture
7. 81112011-0016 Business Planning And Development - Business Modelling
8. 81112011-0017 Business Planning And Development - Enterprise Architecture

C. BUSINESS SOLUTIONS DELIVERY SERVICES

1. 81112011-0018 Business Solutions Delivery - System Analysis and Design
2. 81112011-0019 Business Solutions Delivery - Business Solution Development
3. 81112011-0020 Business Solutions Delivery - Business Solution Certification/Accreditation
4. 81112011-0021 Business Solutions Delivery - Business Solution Maintenance

D. SPECIALISED BUSINESS SOLUTIONS

1. 81112011-0022 Business Solutions Delivery - Specialised - Business Intelligence
2. 81112011-0026 Business Solutions Delivery - Application Configuration Management
3. 81112011-0027 Business Solutions Delivery - Service Delivery (SLA) Management
4. 81112011-0028 Business Solutions Delivery - Capacity Planning and Availability Management

E. INFORMATION SECURITY SERVICES

1. 81112011-0029 Information Security - Security Architecture
2. 81112011-0030 Information Security - Business Continuity Consultancy
3. 81112011-0031 Information Security - Policy Development and Implementation

F. SPECIALISED SECURITY SERVICES

1. 81112011-0032 Information Security - Specialised - Access Control
2. 81112011-0033 Information Security - Specialised - Identity Management
3. 81112011-0034 Information Security - Specialised - Physical and Environmental Security
4. 81112011-0035 Information Security - Specialised - Communication and Operations Security
5. 81112011-0036 Information Security - Specialised - Application Security

	<p>6. 81112011-0037 Information Security - Business Solution Compliance</p> <p>G. BUSINESS SOLUTION IMPLEMENTATION SERVICES</p> <ol style="list-style-type: none"> 1. 81112011-0038 Business Solution Implementation - Application / ICT/COTS Training 2. 81112011-0039 Business Solution Implementation - Training Development and Accreditation 3. 81112011-0040 Business Solution Implementation - Application Deployment Support 4. 81112011-0041 Business Solution Implementation - Organisational Change Management 5. 81112011-0042 Business Solution Implementation - ICT Infrastructure Acquisition Management 6. 81112011-0043 Business Solution Implementation - Operational Procedure Development <p>H. ICT SERVICE SUPPORT MANAGEMENT</p> <ol style="list-style-type: none"> 1. 81112011-0044 ICT Services Support Management - Service Management Centre 2. 81112011-0045 ICT Services Support Management - Service Level Management 3. 81112011-0046 ICT Services Support Management - Problem Management 4. 81112011-0047 ICT Services Support Management - Incident Management 5. 81112011-0048 ICT Services Support Management - ICT Configuration Management 6. 81112011-0049 ICT Services Support Management - Performance and Capacity Management 7. 81112011-0050 ICT Services Support Management - Change and Release Management 	
1.6	ORIGINAL EQUIPMENT MANUFACTURER (OEM) ACCREDITATION	Comply
	<p>The prime bidder confirms to be <u>accredited by the OEM</u> as support partner with the appropriate and <u>relevant certifications</u> for:</p> <ul style="list-style-type: none"> • Antivirus Technology; • Firewall Technologies; • SIEM Technology • Remote Access TechnologiesData Loss Prevention Solutions • Intrusion Detection and Prevention Technologies • Email and Web Filtering Technologies • Cyber Security Technologies <p>Bidders must provide proof of all relevant certification/accreditation as listed above.</p>	

1.7	ABILITY TO DELIVER THE SERVICE TO ALL DOJCD OFFICES WITHIN THE RSA	Comply
	The bidder confirms that, for the duration of the contract, the bidder will have adequate technical competency and capacity to meet all the functional requirements and service level standards within the DOJ&CD.	
1.8	SERVICE LEVEL STANDARDS	Comply
	<p>The bidder accepts the service level standards as stipulated in this document are minimum service levels and that additional service levels can be added during the contract period to optimise the value delivery to the business. The additional service levels and associated penalties will be in line with service levels in the document (e.g. quantum). The added service levels will be in line with the functions stipulated in the contract which may not have specific service level standards.</p> <p>The bidder accepts that a formal Service Level Agreement is to be entered into with the Department, within a period not exceeding 90 days.</p>	
1.9	ISO 27001 CERTIFICATION	Comply
	Provide proof of certification to ISO 27001 – Information Security Management System (ISMS)	
1.10	FULLY COSTED SERVICE	Comply
	<p>The bidder confirms that their bid response is an all-inclusive response that will fully meet all functional requirements, and that will achieve all the purposes, as set out in this document.</p> <p>The bidder confirms that all the requirements and services necessary to deliver the services as set out in this bid document, whether specifically stated or not, are included in the bid price.</p> <p>The bidder is aware and accepts that the cost model provides for composite pricing and does not contain detailed costing elements but confirms that all essential services as determined by the bidder</p>	

	<p>that are required to meet all the requirements of the service have been included in the bid price.</p> <p>The bidder confirms that, after having considered all the requirements of the service</p> <p>that <i>all essential services</i> other than what was stipulated by the Department and <i>that are considered necessary to deliver a composite service from a user and technical perspective</i>, has been included in the bid price.</p> <p>The bidder further confirms that all additional functionality proposed under the Functionality section of this document, have been included in the bid price.</p> <p><i>NB: The bidder confirms that any omission, or oversight in this respect, will be for the bidder's account with no additional cost implications to the Department.</i></p>	
1.11	PENALTIES READ IN CONJUNCTION WITH SECTION 8	Comply
	<ul style="list-style-type: none"> a. If a bidder fails to perform any or all of the service(s) within the agreed timeframes, the Department has the right, without prejudice to its other remedies under the contract, to deduct from the amounts payable, as a penalty, a sum calculated on the percentage under the penalty column levied against the costs or value for non-performance of a particular service definition b. The bidder will not be entitled to any service credits should the service be delivered within or ahead of target timeframes. c. No penalties will be imposed against the bidder in instances where due dates are not met as a result of services that fall outside the scope of the contract with the bidder. d. The enforcement of a penalty does not exempt the bidder from resolving a problem nor does it stop the repetitive levying of the penalty at the stipulated percentage value of a particular service level. The penalty shall be enforced for subsequent periods of non-performance until resolved. e. A maximum penalty principle will be applied when levying penalties for non-performance on the part of the bidder. 	

	<p>Refer to the minimum service level standards section for maximum penalty conditions.</p> <p>f. Service dispute resolution processes may be triggered due to consistent non-performance on the part of the bidder. During a service dispute, the bidder shall continue to render services in accordance with the service levels. In instances where a service dispute arises, the Department undertakes to pay such invoices which are not the subject of the service dispute.</p> <p>g. The Department reserves the right to deduct any penalty amount due, from the next invoice, irrespective of the service to which the penalty applies to.</p> <p>h. Notwithstanding the aforementioned, and without prejudice to any other rights the Department has, the Department reserves the right to enter into dispute resolution process at any point in time with the view of contract cancellation (e.g. service not rendered, unsatisfactory performance, sub-standard work, etc.).</p>	
1.12	FIRM PRICING	Comply
	The bidder confirms that all pricing is firm and that no price adjustments will be applicable or claimed during the contract period, other than CPIX (where applicable and agreed with the Department).	
1.13	COPYRIGHT AND INTELLECTUAL PROPERTY	Comply
	<p>All copyright and Intellectual Property herein vests with DOJ&CD. No part of the contents may be used, copied, disclosed or conveyed in whole or in part to any party in any manner whatsoever other than for preparing a proposal in response to this Bid, without prior written permission from the DOJ&CD.</p> <p>All deliverables (e.g. documents) produced out of the contract will remain the sole intellectual and copyright property of the Department and will only carry the brand (corporate identity) of the Department. No co-branding will be allowed.</p>	

1.14	COSTS INCURRED IN PREPARATION OF RFB RESPONSES	Comply
	The DOJ&CD shall not be liable for any costs incurred by the bidder in the preparation of response to this rfb or to discuss reasons why such bidder's or any other proposal was accepted or rejected.	
1.15	RSA LEGAL ENTITY	Comply
	The prime bidder and it's sub-contractor(s) must be a registered business entity that has its full time operations and capability in South Africa.	
1.16	FUNCTIONALITY - REFERENCING OF SUBSTANTIATIONS	Comply
	Bidders must clearly reference their substantiation in their bid response in specific terms (e.g. reference to schedule, section and page number of their bid response, etc.) The Department will not provide a score for a specific item should the bidder (i) not substantiate their response or (ii) inaccurately reference their response substantiation in their bid response.	
1.17	CLARIFICATION REGARDING RFB AFTER CLOSING DATE	Comply
	The Department may request written clarification regarding any aspect of this proposal (e.g. price confirmation and clarification, verification of certifications, clarification of technical aspects, etc.) The bidders must supply the requested information in writing within the specified time-frames after the request has been made, otherwise the bidder's proposal shall be disqualified.	
1.18	VERIFICATION OF INFORMATION	Comply
	The Department reserves the right to contact any of the references that were provided by the bidder, or to perform its own independent verification to verify information that was provided by the bidder. Where the bidder's permission is required for any reference to release information, whether such reference was provided by the bidder or was obtained through the Department's independent verification process, the bidder shall cooperate to allow such	

	information to be released within the specified timeframes.	
1.19	RIGHT TO CANCEL OR REJECT	Comply
	The DOJ&CD reserves the right to; cancel or reject any proposal and not to award the proposal to the lowest bidder or not to award at all.	
1.20	LIMITATION OF LIABILITY	Comply
	The aggregate liability of the bidder to the Department, whether under the contract, or otherwise, will be equivalent to the total contract price, and shall not apply to the cost of repairing or replacing defective equipment and loss of data.	
1.21	PRINCIPAL AGREEMENTS	Comply
	Where applicable, and during the evaluation process, bidders who are distributors, resellers and installers of equipment and services may be required to submit proof of agreements with their principals (e.g. OEMs). Where such agreements are requested, it shall be valid as from the time of bidding. In the event where a bidder is awarded the bid, the bidder shall ensure that such agreements remain valid for the duration of the contract. The Department reserves the right to validate the authenticity of such agreements, during the evaluation or contract period, in any form deemed necessary.	
1.22	PRECEDENCE OF DOCUMENTS	Comply
	<p>The following order of precedence of documents will apply in concluding the contract and/or SLA:</p> <ol style="list-style-type: none"> 1. The RFB (this document), 2. The Bidder's response 3. Letter of Award 4. The Service Level Agreement (SLA), <p>In case of a conflict between the parties, the conditions of the RFB document will prevail followed by the Bidder's response, followed by the Letter of Award and thereafter SLA (agreed position between the parties).</p>	

1.23	BIDDER'S OWN CONDITIONS	Comply
	<p>Bidders must not qualify the bid with their own conditions.</p> <p>Caution: If the bidder does not specifically withdraw its own conditions when requested by the Department, the bid response will be disqualified.</p>	
1.24	FORMAL CONTRACT	Comply
	<p>The bidder accepts that any offer and/or acceptance entered into will only BE considered valid and binding if reduced in writing.</p> <p>The bidder accepts that any verbal agreement will not constitute a valid contract.</p>	
1.25	DISCRETION TO EXTEND THE VALIDITY PERIOD	Comply
	<p>The DOJ&CD may request for an extension of the validity period.</p> <p>When called upon to extend the validity period, the bidder must respond within the required time-frames and in writing.</p>	
1.26	WITHDRAWAL OF RFB BEFORE VALIDITY EXPIRY	Comply
	<p>Should the bidder withdraw their proposal before the proposal validity expiry date, DOJ&CD reserves the right to recover any additional expenses incurred by DOJ&CD in having to accept any less favourable proposal and/or the additional expenditure incurred by DOJ&CD in the preparation of a new RFB and by the subsequent acceptance of any less favourable proposal.</p>	
1.27	AMENDMENTS TO THIS RFB	Comply
	<p>Any amendment or change of any nature made to this RFB shall only be of force and effect if it is in writing by the Department's designated representative as stipulated in this document.</p>	
1.28	CHANGES TO WORDING OF THE ORIGINAL RFB DOCUMENT	Comply
	<p>Should the bidder change any wording or phrase in this document, the bid shall be evaluated as though no change has been effected and the original wording or phrasing shall be used.</p>	
1.29	NEGOTIATING A FAIR MARKET RELATED PRICE	Comply
	<p>The Department reserves the right to enter into price negotiations with the preferred tenderers before the awarding of the tender.</p>	

1.30	AWARD PROCESS	Comply
	<p>The Department may issue a letter to engage a prospective bidder to commence negotiations (this may include pricing negotiations). The negotiation process may be subject to a predefined timeframe that will be determined by the Department, during which the parties must reach consensus.</p> <p>Where an agreement is not reached within the predefined timeframe, or extended timeframe, the Department reserves the right to close the negotiation process with such a bidder and engage the next bidder.</p>	
1.31	ENFORCEMENT OF PROVISIONS	Comply
	<p>Failure or neglect by either party to (at any time) enforce any of the provisions of this bid shall not, in any manner, be construed to be a waiver of any of that party's rights in that regard and in terms of this bid. Such failure or neglect shall not, in any manner, affect the continued, unaltered validity of this bid, or prejudice the right of that party to institute subsequent action.</p>	
1.32	SECURITY CLEARANCES AND NON-DISCLOSURE AGREEMENTS	Comply
	<p>The bidder will ensure that all its resources involved in the execution of the contract will sign non-disclosure agreements before commencement of contract and shall abide thereby.</p> <p>Employees and subcontractors of the bidders may be required to be in possession of valid security clearances to the level determined by SSA and/or the Department commensurate with the nature of the activities they are involved in.</p> <p>The cost of obtaining suitable clearances is for the account of the bidder. The bidder shall supply and maintain a list (e.g ID numbers, work permit, physical address, etc) of personnel involved on the contract indicating their clearance status, during or after the contracting phase.</p>	

1.33	PARTICIPATION OF OTHER DEPARTMENTS IN THIS CONTRACT	Comply
	The bidder consents that the Department may cede the whole or parts thereof to other Departments/Agencies (e.g. the Office of the Chief Justice), under the same terms and conditions for their own account.	
1.34	INTEREST ON ACCOUNTS IN THE EVENT OF DISPUTES	Comply
	No interest shall be payable on accounts due to the successful bidder in the event of a dispute arising out of any stipulation in the contract.	
1.35	BIDDER'S EXPERIENCE (PRIME BIDDER)	Comply
	The bidder confirms to have experience specifically related to the required services.	
1.36	TRAVELLING, PARKING AND ACCOMMODATION COSTS	Comply
	The bidder accepts that in its discharging of its services, no travelling, parking and accommodation will be reimbursed by the Department. The bidder is required to ensure that all travelling, parking and accommodation costs are included in their pricing and is not costed separately. The Department will not accommodate any claims whatsoever for travelling, parking and accommodation.	
1.37	WORKING HOURS	Comply
	<p>The bidder accepts that working hours is as follows:</p> <ul style="list-style-type: none"> Monday to Friday (excluding public holidays) 07:30 to 17:00 <p>The bidder accepts that in exceptional cases, services may be rendered outside the above working hours (e.g. emergency updates and patches as well as during planned maintenance).</p> <p>The bidder accepts that all required on site resources will be on site as per the department's working hours.</p>	
1.38	AFTER HOURS WORKING	Comply

	The bidder accepts that, where required, services may be performed after hours at no additional cost to the Department (e.g. scheduled maintenance windows, resolutions of major incidents, implementation of emergency updates and patches, etc.).	
1.39	RESOURCES CERTIFICATION & EXPERIENCE	Comply
	<p>a. The bidder accepts that the resources assigned to deliver services to the Department, are certified in line with the functional/technical requirements</p> <p>b. The bidder confirms that the assigned resources meets the minimum requirements as reflected in the RFB.</p> <p>c. The Department reserves the right to request proof of such certification within specified timeframes, as part of compliance to the certification requirements.</p> <p>d. The bidder accepts that all necessary training for their resources (e.g. software version upgrades, existing technology upgrades) is for the bidders own cost. The Department will not accommodate any claims whatsoever for the training of bidders resources.</p>	
1.40	FULL ASSET LIST OF SUPPLIED EQUIPMENT (IF SUPPLIED)	Comply
	<ul style="list-style-type: none"> The bidder shall be required to provide a list of all equipment/artefacts supplied in an electronic format and template prescribed by the Department within 5 days of a request. The minimum Information that the bidder may be required to provide include the following: <ul style="list-style-type: none"> asset serial number, asset tag number, asset name, asset warranty start and end date, exact location of the asset, etc. 	
1.41	USE OF TELEPHONE LINES FOR PERSONAL CALLS	Comply
	The bidder accepts that personal calls made by its resources will be for the account of the bidder.	
1.42	ON SITE RESOURCES	Comply

	All the bidder's onsite resources must be based AT the DOJ&CD National Office in Momentum Building. The Department reserves the right to instruct the bidder to change its onsite resources in the event of unsatisfactory performance, within a period of 2 months.	
1.43	TOOLS OF TRADE	Comply
	The bidder shall provide its own ICT equipment for its resources assigned to the contract (e.g. desktops, laptops)	
1.44	SUPPORT AND SERVICE DESK CONDITIONS	Comply
	<p>a. All service requests will be logged at the Department's ICT Service Desk. The bidder's resources will be given access to the department's service desk application where all queries logged against the application will be assigned to such resources.</p> <p>b. The Department's Service Desk application is the only source of information used to measure adherence to SLA's (e.g. response & resolution times). The bidder may be required to correspond on service requests (e.g. Call status updates) in a manner prescribed by the Department.</p> <p>c. Service requests may be registered through various engagements with the Department's ICT team (e.g. service management meetings); however, these requests must be logged at the Department's ICT Service Desk, prior to implementation.</p>	
1.45	RESOURCE REPLACEMENT	Comply
	In the event that the assigned resource is unavailable, the bidder must ensure that an equivalent replacement resource is provided immediately and inform the Department in writing.	
1.46	BIDDER EXPERIENCE – USER BASE	Comply
	<p>a. The Department has over 20 000 ICT end-users. For the purpose of this bid, bidders must have rendered ICT Security Services as specified in this bid for an organisation with at least 15 000 ICT end-users for a minimum period of at least three (3) years.</p> <p>b. Bidders must provide the following information to confirm the above in the form of a signed reference letter and confirmation that explicitly state at least the following:</p>	

	<ul style="list-style-type: none"> the name of the organisation. the quantity of ICT end-users. The period of the contract. the organisation's relevant contact person and their contact details. Average SLA performance per service over the period of the contract <p>c. The Department reserves the right to verify information with any person/s in the organisations that were provided as reference by the bidder.</p>	
1.47	SOFTWARE LICENSE MANAGEMENT	Comply
	In the event that software licences are overprovisioned by the bidder, without the Department, the bidder accepts that the cost for the overprovisioning will be borne by the bidder.	

SECTION 4: TECHNICAL SPECIFICATIONS FOR APPOINTMENT OF A SERVICE PROVIDER FOR INFORMATION COMMUNICATION TECHNOLOGY (ICT) SECURITY SUPPORT SERVICES FOR A PERIOD OF 3 YEARS

1. INTRODUCTION

- 1.1 The key mandate of the Department of Justice and Constitutional Development (herein after referred to as “the Department”) is to support the administration of Justice and uphold the Constitution. This is achieved through the implementation of an effective and efficient court-based system and the provision of quality legal services to the country’s citizens and the state. In support of these goals, the Department requires well-functioning support services that are in line with best practices and good corporate governance.
- 1.2 In supporting the key mandate of the Department, Information and Communication Technology (ICT) has been identified as one of the key strategic resources and an enabler in continuously improving (modernising) service delivery to the citizens of our country.
- 1.3 To this end, in line with the modernisation journey, the Department has over the years implemented ICT capabilities which include an underlying ICT infrastructure that is required to enable and support business solutions (e.g. core business applications, email, intranet portal, etc.).

2. BID PURPOSE AND SCOPE

- 2.1 The purpose of this bid is to appoint a suitably qualified service provider to provide ICT Security Services for the following service towers and related supporting services: These services are to be provided in line with (i) the defined service level standards (ii) the Department’s processes, and (iii) industry best practices.

2.1.1 ICT Security Operations Management Services - entails the services required to install, configure, support and maintain all IT security related infrastructure software and licences. Furthermore, it entails the services to review, remediate and restore all functional and technical security related incidents and problems emanating from reported security issues in line with the service level agreement (SLA). This is performed using both a proactive

and reactive approach. Incident management will be dealt with on an incident by incident basis and where required and agreed to by the Department, through focussed impactful operational improvement projects.

2.1.2 ICT Security Monitoring and Reporting services – entails the services required to analyse security event data in real time for internal and external threat management purposes and to collect, store, analyze and report on log data for incident response, trend analysis, forensics and regulatory compliance. This will include the setting up and maintaining of the Department's Security Operating Centre. The hardware required for setting up the Department's Security Operating Centre will be provided by the Department either through this contract or a different procurement sourcing model, at the discretion of the Department.

2.1.3 ICT Security Governance, Risk and Compliance Management - entails the services required to secure sensitive information by establishing and developing ICT security processes, policies, risk assessment tools and systems to enable the department to comply with (and complying with the) relevant ICT security standards, legislation and regulations. (as it relates to ICT Security). This includes managing the services related to prevention, mitigation and recovery from a disastrous event impacting on ICT services.

2.1.4 Service Delivery Management services - entails the services required for the overall management of all other service towers and management of ICT Security projects.

2.1.5 Managed Cyber Security Operations Centre (CSOC) – entails.....
offering fully managed Cyber Security Operations Centre (CSOC) services. CSOC must deliver an inclusive cyber security incident detection and response capability. The provider should further provide the Department of Justice and Constitutional Development with a cost-effective solution, offering a team of cybersecurity experts and analysts to detect advanced threats. Moreover, the Managed Threat Detection and Response should deliver value through sophisticated managed detection and response (MDR) service, helping to detect and remediate advanced threats before they impact the business.

The Managed Cyber Security Operations Centre should be able to deliver the following:

Comprehensive 24 hours service x 365 days over the three year period security monitoring:

The Department's systems and applications are residing in a hybrid mix of on-premises and cloud systems.

The CSOC team of cybersecurity experts should monitor data and ICT assets wherever they reside within the organization. Whether the assets are stored in the cloud, on-premises, or both, comprehensive monitoring and review of threats means IT only needs to act when a real threat is identified. CSOC as a service from the provider should include the following benefits:

- Layered Security Monitoring

The provider's approach should include ICT asset discovery, vulnerability assessment, network intrusion detection (NIDS), endpoint detection and response (EDR), and Security Incident Event Management (SIEM) event correlation and log management in one platform.

- Cloud Native

The security monitoring should include cloud-based infrastructure and applications, as well as on-premises environments.

- Centralised Security

The managed CSOC offering should provide comprehensive security, including 24 hours service x 365 days over the three year period threat monitoring, triaging and investigation of incidents, and the use of security orchestration and automation to respond to threats and remediate incidents using pre-built integrations.

- Compliance-minded Security

All security must comply with security standards such as PCI DSS, ISO 27001, SOC 2 Type 2, HIPAA and etc.

- Shared Visibility and Knowledge Transfer

The Department should access and use the very same portal as the Provider's CSOC team, empowering internal IT to work side-by-side on everything from investigations to remediation.

2.1.6 Mimecast (email) Support

The Bidder shall have knowledge and be enabled to support Mimecast wrt the following:

- Manage the Administration Console
- Setup User Interfaces
- Manage Dashboards
- Setup Single Sign On (SSO)
- Configure Mimecast and setup 2 Step Authentication

3. CONTRACT POSITIONING MODEL

- 3.1 For effective management of the contract, the services are to be provided within the context of the Department's governance framework. As such, the diagram below provides an overview of the contract positioning model, and the reporting lines in terms of delivering the various services:

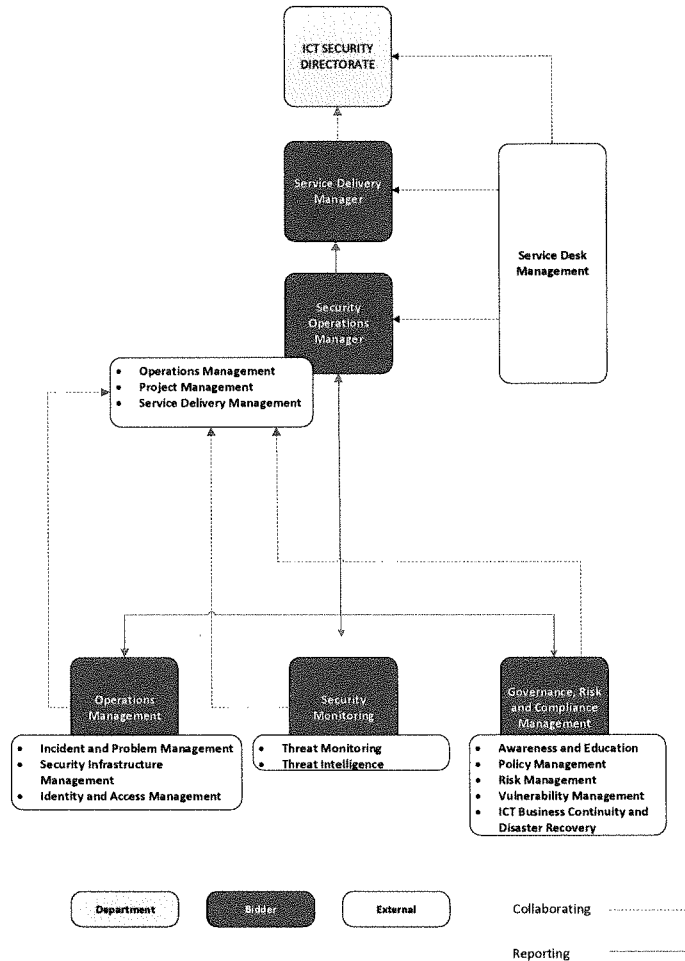


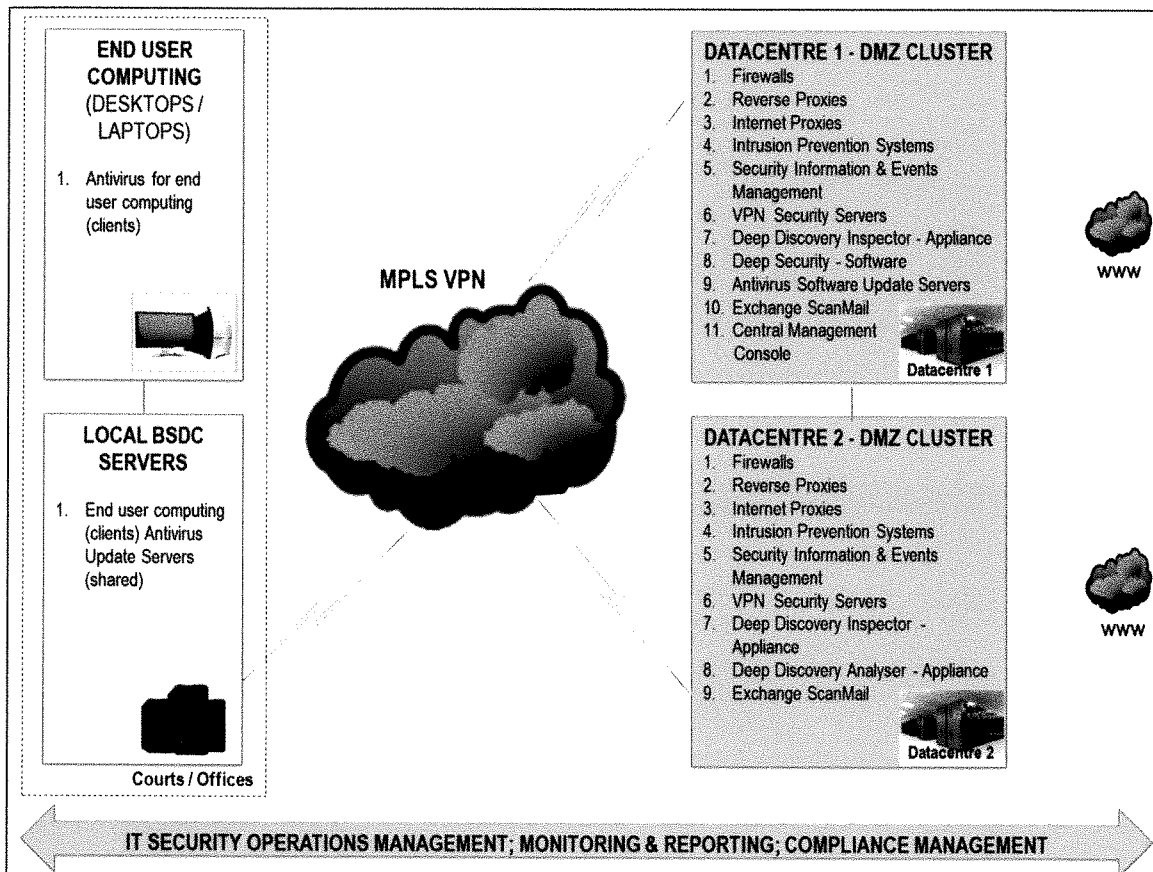
Figure 1: Contract Positioning Model

4. SERVICE OPERATIONS

- 4.1 The Department's Service Desk is the single point of contact for users, where the primary objective of the Service Desk is to restore services within service level standards, with first line call resolutions as the preferred approach. This includes the handling of all communication with the users and ICT stakeholders (e.g. third party suppliers, technical staff).
- 4.2 It is important to note that the Department has outsourced its Service Desk services, and as such the prospective Bidder will be expected to interface with existing service provider for centralized service desk services (e.g. all calls are to be routed via the service desk). Bidder will be expected to perform 1st and 2nd line call resolution as part of maintaining the service standards. This includes making resources available on the service desk dealing specifically with services outlined in this bid.

5. CURRENT IT SECURITY LANDSCAPE

- 5.1 The diagram below provides a high level overview of the current ICT Security landscape in the Department. Detailed information per component contained in the landscape can be found in the table below.



- 5.2 The table below provides detailed information for the hardware and software components as illustrated in the above current IT Security landscape diagram. The quantities provided are based on current data and should be used as reference by bidders in their bid response. It should be noted that these quantities may change in line with the contract scope and contract reduction requirements, as contained in this bid.

ENVIRONMENT	LOCATION	DESCRIPTION	MAKE	MODEL/VERSION	QTY
DATACENTRE 1 – DMZ CLUSTER	CENTURION, GAUTENG	1. Firewalls	Firewall	15600	2
		2. Reverse Proxy	Blue Coat	ProxySG S200-20	1
		3. Internet Proxy	Antivirus Technology	IWSVA 6.5-SP2_Build_Linux_1765	5
		4. Intrusion Prevention Systems	IBM	XGS 5100	2
		5. Security Information & Events Management	IBM	QRadar XGS	2
		6. VPN Security Servers	Microsoft Threat Management Gateway (TMG)	TMG Version 10	1
		7. Deep Discovery Inspector - Appliance	Antivirus Technology	1100	1
		8. Deep Security - Software	Antivirus Technology	10.0.3359	1
		9. Antivirus Software Update Servers	Antivirus Technology	Office Scan; Version 12 XG	11
		10. Exchange ScanMail	Antivirus Technology	9.1.0.1631	2
		11. Central Management Console	Antivirus Technology	Control Manager; Version 7.0 - Build 2442	1
DATACENTRE 2 – DMZ CLUSTER	HARTBEEST POORT, NORTH-WEST PROVINCE	1. Firewalls	Firewall	15600	2
		2. Reverse Proxy	Blue Coat	ProxySG S200-20	1
		3. Internet Proxy	Antivirus Technology	IWSVA 6.5-SP2_Build_Linux_1765	5
		4. Intrusion Prevention Systems	IBM	XGS 5100	2
		5. Netskope	-	-	1
		6. Security Information & Events Management	IBM	QRadar XGS	2
		7. VPN Security Servers	Microsoft Threat Management Gateway (TMG)	TMG Version 10	1
		8. Deep Discovery Inspector - Appliance	Antivirus Technology	1100	1
		9. Deep Discovery Analyser - Appliance	Antivirus Technology	1100	1
		10. Exchange ScanMail	Antivirus Technology	9.1.0.1631	2

ENVIRONMENT	LOCATION	DESCRIPTION	MAKE	MODEL/VERSION	QTY
END USER COMPUTING (DESKTOPS / LAPTOPS)	COUNTRY-WIDE	1. Antivirus for end user computing (clients)	Antivirus Technology	Office Scan; Version 12 XG	20,000
LOCAL BSDC SERVERS	COUNTRY-WIDE	2. End user computing (clients) Antivirus Update Servers	Antivirus Technology	Office Scan; Version 12 XG	650
END USERS	COUNTRY-WIDE	ICT End-Users	n/a	n/a	20,000 (approximately)
IT SECURITY RELATED CALL STATISTICS	COUNTRY-WIDE	Average number of IT Security calls logged per annum (includes incidents, problems, and service requests)	n/a	n/a	2400 (approximately)

6. FUNCTIONAL REQUIREMENTS

- 6.1 In conjunction with the requirements as set out in the Bid Purpose and Scope, the bidder must, amongst others, provide the following generic minimum functional requirements for ICT Security Support Services (including the associated fixed and wireless infrastructure, software configurations and licenses) that are in line with (i) the defined service level standards (ii) the Department's processes, and (iii) industry best practices. These functional requirements apply to *all service towers*:

- 6.1.1 Performing preventative, adaptive and perfective maintenance services.
- 6.1.2 Performing all functions pertaining to CSOC.
- 6.1.3 Managing and resolving all ICT security incidents and problems.
- 6.1.4 Executing all ICT security related changes in accordance with the Department's change management processes.
- 6.1.5 Performing all functions pertaining to ICT security service Availability Management.
- 6.1.6 Performing all functions pertaining to ICT security service Capacity Management.
- 6.1.7 Performing all functions pertaining to ICT security service Performance Management – in line with an acceptable threshold of <7 seconds response times.

- 6.1.8** Ensuring that the ICT security infrastructure layer and its configuration information is accurately captured on the Configuration Management Data Base (CMBD), throughout its lifecycle.
- 6.1.9** Performing all functions pertaining to the management (including engagements) of third party suppliers, via the Departments Service Desk partner (Vendor Management).
- 6.1.10** Producing the necessary reports (e.g. trend analysis, service performance) for service improvement and management reporting purposes.
- 6.1.11** Ensuring that the infrastructure layer management toolsets provided by the Department meet the service requirements by recommending improvements in the toolset configuration to the Department.
- 6.1.12** Participating in performing all backups related to ICT security management systems.
- 6.1.13** Building and maintaining standard image stacks as it relates to ICT security management.

6.2 Service Towers

In addition to the aforementioned functional requirements the following service towers are to be provided and supported in line with (i) service level standards, (ii) Departmental processes, and (iii) industry best standards.

6.2.1 ICT Security Operations Management Services

- i. perform all functions related to 1st and 2nd line support of the ICT security infrastructure and services,
- ii. managing all the ICT Security Infrastructure, Software and Licences.
- iii. managing endpoint (desktops, laptops, server's mobile devices) security. (antivirus, encryption, security patches, etc.).
- iv. managing network security and related services (e.g. VPN, MPLS, IIS, Internet, SSL certificates, Intranet, etc.).
- v. manage application security (in collaboration with application owners and third party vendors).
- vi. manage identity and logical access.
- vii. managing ICT security incidents, threats and events.
- viii. managing ICT security problems.
- ix. managing the fulfilment of ICT security service requests.

- x. managing ICT security changes in line with the Department's change management processes.
- xi. managing ICT security releases and deployments in line with the Department's release management processes.
- xii. engaging and communicating between all technical teams and all stakeholders (including ICT end-users).
- xiii. ensuring that, subject to approval from the Departments delegated authority, all ICT security management related software is one version below the latest version of the OEM (n-1), with the latest version (n) being preferred, except in instances where the Department elects to remain with an older version of the software due to known constraints.
- xiv. providing overall leadership and management for all ICT security services provided by the successful bidder.
- xv. ensuring that all documentation for all the services are in place and are continuously updated to reflect the current status.
- xvi. providing overall service level management for all the services.
- xvii. ensuring that all the toolsets provided by the Department meet the service requirements by recommending improvements in the toolset configuration to the Department.
- xviii. managing the overall finances (e.g. invoices, invoice reconciliations) for all the services provided.
- xix. providing standard technical and executive management reports on a daily, weekly, monthly and annual basis, including on an ad-hoc basis as required.
- xx. participating in ICT security services review meetings as conducted by the Department.
- xxi. coordinating and managing all communication and engagements with all required stakeholders (e.g. during resolution of major incidents and problems).
- xxii. reviewing and updating the Department's ICT security strategy and implementation plan in conjunction with the relevant unit within the Department.
- xxiii. reviewing and updating the Department's ICT security policies and procedures in conjunction with the relevant unit within the Department.
- xxiv. documenting, reviewing and updating the Department's overall ICT security architecture.

- xxv. reviewing all architectural designs (ICT infrastructure and ICT business applications) as it relates to the security aspects of these architectures.
- xxvi. managing ICT Security projects.

6.2.2 ICT Security Monitoring and Reporting Services

- i. proactively monitoring, analysing and reporting on ICT security threats, incidents and events.
- ii. performing and managing ICT security vulnerability assessments.
- iii. proactively monitoring, analysing and reporting on ICT security patches and updates.
- iv. performing trend analysis and reporting on monitoring activities.
- v. proactively and reactively managing the utilisation and allocation of all ICT security related software licenses (ICT security infrastructure and ICT end-users).
- vi. monitoring and reporting on all ICT security related software licences (ICT security infrastructure and ICT end-users) and informing the Department on the utilization of software licenses once a specific threshold is reached. In the event that software licences are overprovisioned by the successful bidder, without having formally notified the Department, the successful bidder will be held liable for the cost of the software licence overprovisioning.

6.2.3 ICT Security Governance, Risk and Compliance Management

- i. assessing, reporting and ensuring compliance to relevant legislation and regulations as it relates to ICT security.
- ii. developing and maintaining information ICT security policies, procedures, standards and guidelines in line with industry best practices, regulatory and government wide frameworks.
- iii. developing electronic material required for conducting ICT security awareness programs (e.g. training and communication material).
- iv. performing user education and awareness training where required.
- v. assessing and documenting ICT security risks mitigation implementation action plans.

- vi. manage and test the Department's approved ICT Business Continuity/ Disaster Recovery plans.
- vii. Providing inputs and reports to the ICT Security Management Forum on a monthly basis.
- viii. Attend the scheduled contract management meetings.

7. SERVICE LEVELS AND PENALTIES

- 7.1 The tables below stipulate the minimum service levels, targets and penalties that will apply for each Service Tower
- 7.2 A maximum penalty of 30% per month will be applied when levying penalties for non-performance for each service tower in terms of the pricing schedule.
- 7.3 The Department reserves the right to terminate the contract should penalties be levied for 30% on any service description for three consecutive months for each service tower.
- 7.4 Monthly SLA reviews will be conducted to discuss performance, non-performance and compliance.

7.4.1 ICT Security Operations Management services

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
ICT Security Operations Management services (including CSOC/SIEM)	Incidents: Break-fix (day-to-day related incidents)	1 hour	8 hours	98% of all calls resolved within SLA timeframes.	10% of the monthly IT Security Operations Management tower cost.
	Incidents: Break-fix (threats and security breaches related)	1 hour	4 hours	98% of all calls resolved within SLA timeframes.	10% of the monthly IT Security Operations Management tower cost.

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
	Incidents: Call resolution quality (includes day-to-day incidents, security breaches, threats)	n/a	n/a	98% of all incidents not re-opened after resolution (including incidents related to a problem).	10% of the monthly IT Security Operations Management tower cost.
	Service requests: Call resolution quality	n/a	n/a	98% of all service requests not re-opened after resolution.	10% of the monthly IT Security Operations Management tower cost.
	Problem Management and Major Security Incidents: Root Cause Analysis Report (includes problems and major incidents arising out of day-to-day incidents, security breaches, threats)	1 hour	40 hours	100% of all Root Cause Analysis reports provided within SLA timeframes.	10% of the monthly IT Security Operations Management tower cost.
	Problem Management and Major Security Incidents: Root Cause Analysis recommendation implementation (includes problems and major incidents arising out of	n/a	n/a	100% of all Root Cause Analysis approved recommendations implemented within agreed timeframes.	15% of the monthly IT Security Operations Management tower cost.

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
	day-to-day incidents, security breaches, threats)				
	Patch implementation management	n/a	n/a	98% of all approved patches implemented within approved timeframes.	15% of the monthly IT Security Operations Management tower cost.
	Install, Move, Decommission (IMD operations)	1 hour	16 hours	98% of all calls resolved within SLA timeframes and in accordance to change management process. The SLA will start after the change had been approved.	10% of the monthly IT Security Operations Management tower cost.
	Installing and configuring all IT Security Infrastructure, Software and Licences	n/a	As per agreed timeframes	100% of all installations and configurations completed as per agreed timeframes.	10% of the monthly IT Security Operations Management tower cost.
	Availability	n/a	n/a	99% infrastructure uptime.	10% of the monthly IT Security Operations Management tower cost
	Performance Management: Overall performance management.	n/a	daily, weekly, monthly, annually	100% of all performance management reports (including analysis and recommendations) provided	10% of the monthly IT Security Operations Management tower cost

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
				within agreed SLA timeframes.	
	Reporting	n/a	daily, weekly, monthly, annually	100% of all reports provided within agreed SLA timeframes.	10% of the monthly IT Security Operations Management tower cost
	All on site resources at work as per stipulated working hours.	n/a	n/a	100% of all on site resources at work as per stipulated working hours.	10% of the monthly IT Security Operations Management tower cost

7.4.2 ICT Security Monitoring and Reporting

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
ICT Security Monitoring and Reporting (including CSOC/SIEM)	Incidents and Problems – Continuous Scanning & Analysis	n/a	n/a	100% of Incidents and Problems continuously Scanned and Analysed on a daily basis.	10% of the monthly IT Security Monitoring and Reporting tower cost.
	Incidents and Problems - Scanning & Analysis Reporting	n/a	1 hours	100% of all incidents and problems identified as security breaches and/or threats logged.	10% of the monthly IT Security Monitoring and Reporting tower cost.
	Vulnerability Assessment – performing tests & reporting	n/a	Four (4) Vulnerability Assessment Test and Reporting completed per annum.	100% of Vulnerability Assessment Test and Reporting completed per annum for the duration of the contract. Period of	10% of the quarterly (3 months) IT Security Monitoring and Reporting tower cost.

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
				tests and reports submitted to be every three (3) months.	
	IT Security Patches - Monitoring & Analysis & Reporting	n/a	Daily analysis & reporting and Monthly consolidated reporting.	IT Security Patches Analysis & Reporting performed on a daily basis with reporting consolidated on a monthly basis.	10% of the monthly IT Security Monitoring and Reporting tower cost.
	Deep Security Monitoring - Analysis & Reporting	n/a	Daily analysis & reporting and Monthly consolidated reporting.	Deep Security Monitoring - Analysis & Reporting performed on a daily basis with reporting consolidated on a monthly basis.	10% of the monthly IT Security Monitoring and Reporting tower cost.
	IT Security related Software Licence management: compliance to the Department's software license agreements and volume baselines.	n/a	n/a	100% compliance to the Department's software license agreements and volume baselines. Successful bidder will be held liable for the cost of the software licence overprovisioning.	Cost of the overprovisioned software licences as per asset reconciliation.
	Overall Tower - Performance Management: Overall performance management.	n/a	daily, weekly, monthly, annually	100% of all performance management reports (including analysis and recommendations) provided within agreed SLA timeframes.	10% of the monthly IT Security Monitoring and Reporting tower cost.

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
	Overall Tower - Reporting	n/a	daily, weekly, monthly, annually	100% of all reports provided within agreed SLA timeframes.	10% of the monthly IT Security Monitoring and Reporting tower cost.
	Overall Tower - All on site resources at work as per stipulated working hours.	n/a	n/a	100% of all on site resources at work as per stipulated working hours.	10% of the monthly IT Security Monitoring and Reporting tower cost.

7.4.3 ICT Security Governance, Risk and Compliance Management

SLA Type	Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
IT Security Compliance Management (including CSOC/SIEM)	Compliance to relevant ICT Security Legislation and Regulations -	n/a	Four (4) compliance assessment reports per annum.	100% of compliance assessment reports completed per annum for the duration of the contract. Period of assessments and reports submitted to be every three (3) months.	10% of the quarterly (3 months) IT Security Compliance Management tower cost.
	ICT Security related Policies, Procedures, Standards, Guidelines - Development	n/a	n/a	As per agreed timelines.	10% of the monthly IT Security Compliance Management tower cost.
	ICT Security related Policies, Procedures, Standards, Guidelines –	n/a	n/a	100% of IT Security Policies, Procedures, Standards, Guidelines continuously	10% of the monthly IT Security Compliance Management tower cost.

SLA Type	Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
	Upkeep and alignment to current operations.			updated and aligned to reflect current operations.	
	ICT Security related Policies, Procedures, Standards, Guidelines – Major Review	n/a	n/a	As per agreed timelines.	10% of the monthly IT Security Compliance Management tower cost.
	ICT Security Awareness Programs – Material Development (electronic format)	n/a	n/a	As per agreed timelines.	10% of the monthly IT Security Compliance Management tower cost.
	ICT Security Risks – assessment and reporting	n/a	n/a	Monthly IT Security Risks assessment and reports completed.	10% of the monthly IT Security Compliance Management tower cost.
	ICT Security Risks – mitigation implementation	n/a	n/a	As per agreed timelines.	10% of the monthly IT Security Compliance Management tower cost.
	Overall Tower - Performance Management: Overall performance management.	n/a	daily, weekly, monthly, annually	100% of all performance management reports (including analysis and recommendations) provided within agreed SLA timeframes.	10% of the monthly IT Security Compliance Management tower cost.
	Overall Tower - Reporting	n/a	daily, weekly,	100% of all reports provided within	10% of the monthly IT Security

SLA Type	Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
			monthly, annually	agreed SLA timeframes.	Compliance Management tower cost.
	Overall Tower - All on site resources at work as per stipulated working hours.	n/a	n/a	100% of all on site resources at work as per stipulated working hours.	10% of the monthly IT Security Compliance Management tower cost.

7.4.4 Service Delivery Management

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
Service Delivery Management Services	Overall processes, procedures and documentation – central repository	n/a	5 days after document sign-off	100% of all processes, procedures and documentation stored in the Department's documentation repository.	10% of the monthly Service Delivery Management tower cost.
	Overall Service - Performance Improvement Plans	n/a	4 reports per annum	100% of all Performance Improvement Plans completed. Period of plans submitted to be every three (3) months.	10% of the quarterly (3 months) Service Delivery Management tower cost.
	Finance management (e.g. invoices)	n/a	80 hours	100% of all invoices due submitted ten (10) days after month end.	No financial penalty, however, service disputes may be imposed by the Department, should this service standard not be achieved.
	Overall Reporting (executive management reports)	n/a	weekly, monthly, quarterly, annually	100% of all reports provided within agreed SLA timeframes.	10% of the monthly Service Delivery Management tower cost.

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
	Department's ICT Security Strategy & Plan – drafting, reviewing and updating (including CSOC/SIEM)	n/a	Finalised first draft completed within 6 months of contract commencement date. Quarterly review performed (every 3 months)	Finalised first draft within 6 months of contract commencement date and Quarterly review performed (every 3 months).	10% of the monthly Service Delivery Management tower cost.
	Department's Overall ICT Security Architecture – documenting (including CSOC/SIEM)	n/a	Finalised first draft completed within 1 month of contract commencement date.	As per agreed timelines.	10% of the monthly Service Delivery Management tower cost.
	Department's Overall IT Security Architecture – reviewing and updating (including CSOC/SIEM)	n/a	Monthly review performed.	Department's Overall IT Security Architecture continuously updated and aligned to reflect current operations on a monthly basis.	10% of the monthly Service Delivery Management tower cost.
	Other Architectural Designs (e.g. infrastructure and business applications) – review of ICT Security aspects only (including CSOC/SIEM)	n/a	n/a	As per agreed timelines.	10% of the monthly Service Delivery Management tower cost.
	Stakeholders Coordination & Management – communication and engagements	n/a	n/a	100% of all stakeholders communicated and engaged with as required (e.g. during major incidents and problems)	10% of the monthly Service Delivery Management tower cost.

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Targets	Penalty
	Service Management: Supported application Performance ICT Security Services must at all times conform, or contribute to achievement of performance threshold of seven (7) seconds or less.	n/a	Daily, weekly, monthly	<7 seconds overall response time (per screen transition) for all supported business applications and related services.	10% of the monthly Service Delivery Management tower cost.
	Overall Tower - All on site human resources at work as per stipulated working hours.	n/a	n/a	100% of all on site resources at work as per stipulated working hours.	10% of the monthly Service Delivery Management tower cost.

8. PROJECTS

8.1 For the purposes of this bid, projects are regarded as initiatives that will be implemented in the various service towers to achieve a specific business value in a focussed way. Projects are unique in that they have a specific scope (goal), timeframe and cost. These projects will be implemented by a different team from the day-to-day support and maintenance team. Projects are categorised as follows:

8.1.1 Defined Projects, and

8.1.2 Ad-hoc projects.

8.2 **Defined Projects** – these relates to projects that are known at the time of the bid, and the bidder is expected to plan and cost for its implementation as part of the bid response.

8.3 **Ad- hoc Projects** – this relates to projects that are not known at the time of publishing the bid, and might arise during the lifetime of the contract. Bidders are not to plan for and cost for these, and the amount included in the cost model for projects is the ceiling amount allocated by the Department for the duration of the contract and is not an

amount that is payable or accrued to the successful bidder. It is therefore not guaranteed that the full amount will be utilised during the contract period.

8.4 **Defined Projects**. The following projects are known, and ARE expected to be executed during the lifetime of the contract:

8.4.1 **Transitioning-In Services**, which will be will be implemented for a period of one (1) month starting a week after the signing of the contract award by all parties (signing of the contract award entails the Letter of Award and not the purchase order which will be issued in due course) and includes, amongst others, the following:

- i. providing transitioning-in services at the commencement of the contract period.
- ii. providing a detailed plan (including roles and responsibilities of the bidder, the Department and the current service provider) with timeframes on how transitioning-in services will be provided.
- iii. ensuring that during the transitioning-in period all tasks are implemented in line with the agreed plan between the Department and the successful bidder.
- iv. ensuring that no services are disrupted during the transitioning-in period.
- v. working alongside the Department and the outgoing Service Provider during this period to ensure a smooth transition of services and business continuity.

8.4.2 **Transitioning-Out services**, which will BE implemented for a period of one (1) month before the end of the contract termination date and includes, amongst others, the following:

- i. providing transitioning-out services at the end of the contract period.
- ii. providing a detailed plan (including roles and responsibilities of the bidder, the Department and the new service provider) with timeframes on how transitioning-out services will be provided.
- iii. ensuring that during the transitioning-out period all tasks are implemented in line with the agreed plan between the Department and the bidder.

- iv. ensuring that no services are disrupted during the transitioning-out period.
- v. working alongside the Department and the incoming Service Provider during this period to ensure a smooth transition of services and business continuity.

8.5 Service Level Standards: The tables below stipulate the service levels, targets and penalties that will apply for project management services. A maximum penalty of 30% per month will be applied when levying penalties for non-performance.

8.5.1 Generic Service Levels and Penalties (applicable to all projects)

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Overall Target	Penalty
Projects Services	Projects - issuing of statement of work authorisations	1 day	10 days	100% of all statement of work authorisations issued within SLA timeframes.	5% of the value of the statement of work authorisation.
	Projects - implementation management	n/a	n/a	100% of all projects implemented in line with the approved statement of work (scope, timeframes, cost) and Departmental Project Management Framework.	10% of the value of the statement of work authorisation.
	Projects - documentation	n/a	n/a	100% of all projects documentation stored in the Department's project documentation repository.	10% of the value of the statement of work authorisation.
	Projects Financial Management (e.g. invoices)	n/a	Project invoices – within agreed timeframes	100% of all invoices due submitted within agreed timeframes.	No financial penalty, however, service disputes may be imposed by the Department,

SLA Type	Service Description	Mean Time To Respond	Mean Time To Resolve	Overall Target	Penalty
					should this service standard not be achieved.
	Projects - status reporting (e.g. project status reporting)	n/a	In line with the Project Implementation Plan	100% of all reports provided within agreed SLA timeframes.	10% of the monthly Service Delivery Management tower cost.

8.5.2 Service Levels and Penalties: Contract Transition-in and Contract Transition-out

SLA Type	Description	Mean Time To Respond	Mean Time To Resolve	Overall Target	Penalty
Transitioning-In services	Provision of an updated detailed plan (including roles and responsibilities of the bidder, the Department and the current service provider) with timeframes on how Transitioning-In services will be provided.	1 day	5 days	Updated detailed plan issued within SLA timeframes. (bidders are required to provide original detailed plans for transitioning-in and transitioning-out services as part of their bid response in line with technical functionality evaluation requirements)	5% of the Transitioning-in services amount.
	Transitioning-in services - implementation	n/a	1 month, starting a week after the signing of the contract award by all parties. (Letter of	100% of Transitioning-In services implemented in line with the approved plan.	15% of the Transitioning-In services amount.

SLA Type	Description	Mean Time To Respond	Mean Time To Resolve	Overall Target	Penalty
			Award and not the purchase order which will be issued in due course)		
Transitioning-Out services	Provision of a detailed plan (including roles and responsibilities of the bidder, the Department and the current service provider) with timeframes on how Transitioning-Out services will be provided	1 day	10 days	Detailed Plan issued within SLA timeframes	5% of the Transitioning-Out services amount.
	Transitioning-Out services - implementation	n/a	1 month before the end of the contract termination date	100% of Transitioning-out services implemented in line with the approved plan.	15% of the Transitioning-Out services amount.

9. HUMAN RESOURCES REQUIREMENTS

- 9.1 The bidder must ensure that, for the duration of the contract, adequate and certified resources are made available to deliver the required functions within the stipulated service level standards, taking into consideration the expected business outcomes, the functional requirements, the size of the organization's overall ICT environment, ICT Security environment and industry best practices. Therefore, the bidder must ensure that, at a minimum, the following types and quantities of resources are provided as (i)

onsite on a full time basis and (ii) as and when required (iii) Centre of Excellence resources and services, as specified in the table below:

Service Tower	Title	Resource Location	Qty	Function
Security Operations Management	Firewall and Proxy Specialist	Required onsite as and when required	n/a	All functions as it relates to the services as stipulated in the bid. These services include the designing, implementing, supporting, maintaining and monitoring of all services, including all hardware and associated software.
	Firewall and Proxy Engineer	Onsite on a full time basis	1	
	Internet Security Specialist	Onsite on a full time basis	1	
	Junior Internet Security Engineer	Onsite on a full time basis	1	
	Trend Micro Senior Specialist	Onsite on a full time basis	1	
	ICT Security Engineers	Onsite on a full time basis	2	
	Cloud Email Specialist	Onsite/Remote on a full time basis	1	
ICT Security Monitoring and Reporting	Senior ICT Security Monitoring Analyst	Onsite on a full time basis	1	
	Junior ICT Security Monitoring Analyst	Onsite on a full time basis	1	
ICT Security Governance, Risk and Compliance Management	Senior ICT Security Governance Compliance & Risk Manager	Onsite on a full5 time basis	1	
Service Delivery Management	Service Delivery Management representative	Onsite on a full time basis	1	

SECTION 5: TECHNICAL EVALUATION : FUNCTIONALITY PHASE

1. CONDITION FOR EVALUATION

- 1.1 Bidders must comply with this section as they form the basis for scoring a bidder's proposal. In order for a bidder to qualify to be evaluated for functionality, a bidder must not have been disqualified on compliance with any prequalifying conditions or mandatory requirements preceding this phase of the evaluation.
- 1.2 The bid will be evaluated in four (4) phases:
- 1.2.1 SCM Pre-Qualification Criteria
 - 1.2.2 Technical Mandatory Requirement
 - 1.2.3 Technical Functional Criteria
 - 1.2.4 Price and B-BBEE
- 1.3 A panel representing the Department will evaluate the proposals received according to the set evaluation criteria. In respect of the evaluation matrix, the prospective service bidders will be rated from 0 to 3 in that:

Score	Meaning	Explanation
0	○ Non responsive	<ul style="list-style-type: none">• Not relevant, no evidence / no information / no inputs
1	○ Poor response	<ul style="list-style-type: none">• Meets some, but not all of the minimum requirements.• Evidence not enough to substantiate the requirement.
2	○ Good response	<ul style="list-style-type: none">• Fully meets and complies with the specification requirements.• Evidence substantiates the requirements.
3	○ Excellent response	<ul style="list-style-type: none">• Fully meets and complies with the specification requirements.• Evidence substantiates the requirement.• Additional innovation, best practice standards, benchmark models and better service offerings provided.

- 1.4 In order to ensure meaningful participation and effective comparison, bidders are requested to furnish detailed information in substantiation of compliance to the evaluation criteria.

- 1.5 Bidders that score less than seventy **70 points / %** in respect of functionality compliance will be regarded as non-responsive and will not be evaluated further.
- 1.6 The following items will be evaluated and scored. Bidders must substantiate each aspect of their response. Bidders must clearly reference their substantiation in their bid response in specific terms (e.g. reference to schedule, section and page number of their bid response, etc.).

Criteria	Rating Matrix						%
	0	1	2	3	4	5	Weight
Overall Bidder Experience							20%
Bidder Human Resources Experience							20%
IT Security Operations Management							15%
IT Security Monitoring and Reporting							20%
IT Security Governance, Risk and Compliance Management & Service Delivery Management							15%
IT Security Contract Transition-in and Contract Transition-out							10%
TOTAL							100%

TECHNICAL EVALUATION FUNCTIONALITY SCORING - RATINGS

1.1.1	Overall Bidder Experience	20%														
	<p>In view of the functional requirements, the size of the organization's ICT environment, the number of and geographically distributed nature of the Department's offices, and the stipulated service level standards, describe, taking into account all the information provided in the specifications, your organisations experience (minimum of three (3) years at an organization of at least 15 000) relating to the following Service Towers:</p> <ul style="list-style-type: none"> ○ IT Security Operations Management (hardware and software) ○ IT Security Monitoring and Reporting (hardware and software) ○ IT Security Governance, Risk and Compliance Management (hardware and software) ○ Service Delivery Management Services <p>1.1.1.1 Briefly describe your organisation(s) experience relating to the service towers as stipulated in this RFB.</p> <table border="1" style="margin-left: 40px;"> <thead> <tr> <th>Score</th> <th>Total Years of Relevant Experience</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>No relevant experience</td> </tr> <tr> <td>1</td> <td>Less than 3 years</td> </tr> <tr> <td>2</td> <td>3 years</td> </tr> <tr> <td>3</td> <td>More 3 years</td> </tr> </tbody> </table> <p>1.1.1.2 Please indicate in which customer organisations you have successfully provided the above services. Your response must include:</p> <ul style="list-style-type: none"> ○ the name of the organisation (a maximum of 3) ○ Name of the project ○ Quantity of ICT end-user within the customer organisation ○ Cost of the project ○ Period of the contract ○ Average SLA performance per service over the period of the contract ○ the organisations relevant contact person and their contact details. ○ Annexure A must be completed <table border="1" style="margin-left: 40px;"> <thead> <tr> <th>Score</th> <th>No. of relevant Customer Organisations</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>		Score	Total Years of Relevant Experience	0	No relevant experience	1	Less than 3 years	2	3 years	3	More 3 years	Score	No. of relevant Customer Organisations		
Score	Total Years of Relevant Experience															
0	No relevant experience															
1	Less than 3 years															
2	3 years															
3	More 3 years															
Score	No. of relevant Customer Organisations															

0	No relevant customer organisations
1	1 relevant customer organisation
2	2 relevant customer organisations
3	3 or more customers

The Department, reserves the right, if required, to contact these organisation to verify the information provided during the functional evaluation phase.

Information provided in this section will be evaluated based on relevant experience of the primary bidder(s), its subcontractor(s) or the combined experience of the bidder(s) (Consortium or Joint Venture) and subcontractors(s).

Have you (the bidder) substantiated your response?	YES	NO
---	------------	-----------

Indicate the corresponding paragraph that specifically substantiates responses in your bid response.	
---	--

1.1.2	Bidder Human Resources Experience	20%									
	<p>One of the critical success factors of delivering these services is the Human Resources that are assigned to deliver services in this contract. The accreditation of the resources in the relevant technologies is important in ensuring optimal services to meet the requirements and the stipulated service levels. All the full time resources allocated to the project must be based at the Department's premises on a full time basis. If the resource is not available for a consecutive period of one week or more, an equivalent resource must be made available at no additional cost to the Department.</p> <p>Taking into account all the information provided in the specifications, please provide the following:</p> <p>1.1.2.1 The organogram including all resources that will be allocated full time to the project.</p> <p>1.1.2.2 A separate organogram including any other resources that will support the team on site and will be made available when required (e.g. major incidents, architecture designs, etc).</p> <p>1.1.2.3 A complete list of Human Resources that must be assigned, to the contract, on a full time basis and demonstrate qualification and competence of key staff in relation to the applicable scope of work. The following details are required:</p> <ul style="list-style-type: none"> ○ Name of the resource ○ Resource qualifications ○ Resource experience ○ Name of organisation(s) where projects were implemented ○ Name of the projects implemented ○ Duration of the project <p>Annexure B must be completed only for full-time resources allocated to the contract.</p> <ul style="list-style-type: none"> ○ Please attach certificates in respect of each of the full-time resources indicated in Annexure B¹ (please note that you can provide additional certificates to the listed) <table border="1" data-bbox="336 1576 1444 1953"> <thead> <tr> <th data-bbox="336 1576 783 1621">Requirements</th><th data-bbox="791 1576 1169 1621">Criteria</th><th data-bbox="1177 1576 1444 1621">Score</th></tr> </thead> <tbody> <tr> <td data-bbox="336 1632 783 1711">Primary Human Resource Requirements</td><td data-bbox="791 1632 1169 1711">Comply with all requirements</td><td data-bbox="1177 1632 1444 1711"></td></tr> <tr> <td data-bbox="336 1722 783 1953">Critical Human Resource Profile</td><td data-bbox="791 1722 1169 1953"> <ul style="list-style-type: none"> • Resource(s) Qualifications(max 3) • Resource(s) Experience(min 3 years) </td><td data-bbox="1177 1722 1444 1953"></td></tr> </tbody> </table>		Requirements	Criteria	Score	Primary Human Resource Requirements	Comply with all requirements		Critical Human Resource Profile	<ul style="list-style-type: none"> • Resource(s) Qualifications(max 3) • Resource(s) Experience(min 3 years) 	
Requirements	Criteria	Score									
Primary Human Resource Requirements	Comply with all requirements										
Critical Human Resource Profile	<ul style="list-style-type: none"> • Resource(s) Qualifications(max 3) • Resource(s) Experience(min 3 years) 										

Project Profile	<ul style="list-style-type: none"> Name of projects implemented(max 5) Name of organisation(s) where projects were implemented (max 5) 	
separate organogram	<ul style="list-style-type: none"> Submission of separate of organogram Demonstration of reserve capacity in the event of a major incidence 	

Score	Meaning	Explanation
0	○ Non responsive	•Not relevant, no evidence / / no information / no inputs
1	○ Poor response	<ul style="list-style-type: none"> Meets some, but not all of the minimum requirements. Evidence not enough to substantiate the requirement.
2	○ Good response	<ul style="list-style-type: none"> Fully meets and complies with the specification requirements. Evidence substantiates the requirements.
3	○ Excellent response	<ul style="list-style-type: none"> Fully meets and complies with the specification requirements. Evidence substantiates the requirement. Additional innovation, best practice standards, benchmark models and better service offerings provided.

Have you (the bidder) substantiated your response?	YES	NO
Indicate the corresponding paragraph that specifically substantiates responses in your bid response.		

1.1.3	ICT Security Operations Management	15%															
	<p>The objective of the Department's ICT Security Operations Management entails the services required to install, configure, support and maintain all ICT security related infrastructure software and licences. Furthermore, it entails the services to review, remediate and restore all functional and technical security related incidents and problems emanating from reported security issues.</p> <p>Taking into account all the information provided in the specifications, describe:</p> <p>1.1.3.1 In general, how will you meet all requirements of the ICT Security Operations Management within the stipulated service level standards utilising all specified toolsets?</p> <p>1.1.3.2 Specifically, how will you utilise Deep Security technology to improve security in the ICT environment in the Department.</p> <p>1.1.3.3 Specifically, how will you implement effective Patch Management in the environment.</p> <p>1.1.3.4 Specifically, how will you manage Availability of Services within the stipulated service level standards?</p> <p>1.1.3.5 Specifically, how will you manage Cyber Security Services and Technology to improve security in the ICT environment in the Department.</p> <p>1.1.3.6 How will you manage 1st, 2nd and 3rd line support?</p> <table border="1"> <thead> <tr> <th>Score</th><th>Meaning</th><th>Explanation</th></tr> </thead> <tbody> <tr> <td>0</td><td>○ Non responsive</td><td>•Not relevant, no evidence / / no information / no inputs</td></tr> <tr> <td>1</td><td>○ Poor response</td><td>• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.</td></tr> <tr> <td>2</td><td>○ Good response</td><td>• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.</td></tr> <tr> <td>3</td><td>○ Excellent response</td><td>•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.</td></tr> </tbody> </table>		Score	Meaning	Explanation	0	○ Non responsive	•Not relevant, no evidence / / no information / no inputs	1	○ Poor response	• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.	2	○ Good response	• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.	3	○ Excellent response	•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.
Score	Meaning	Explanation															
0	○ Non responsive	•Not relevant, no evidence / / no information / no inputs															
1	○ Poor response	• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.															
2	○ Good response	• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.															
3	○ Excellent response	•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.															
	<p>Have you (the bidder) substantiated your response?</p>	<p>YES NO</p>															
	<p>Indicate the corresponding paragraph that specifically substantiates responses in your bid response.</p>																

1.1.4	IT Security Monitoring and Reporting		20%															
<p>One of the most important requirements for the Department's IT Security Monitoring and Reporting is to analyze security event data in real time for internal and external threat management, and to collect, store, analyze and report on log data for incident response, forensics and regulatory compliance.</p> <p>Taking into account all the information provided in the specifications, describe:</p> <p>1.1.4.1 In general, how will you meet all functional requirements of the IT Security Monitoring and Reporting tower within the stipulated service level standards?</p> <p>1.1.4.2 Specifically, how will you conduct the required IT Security Vulnerability assessments every 3 months (quarterly)?</p> <p>1.1.4.3 Specifically, how will you utilise the Security Incidents and Event Management (SIEM) processes and toolsets provided.</p> <p>1.1.4.4 Specifically, how will you utilise Deep Security monitoring, trend analysis and reporting to improve the security of the ICT environment?</p> <p>1.1.4.5 Specifically, how will you monitor and report on Cyber Security Services and Technology utilisation to improve security in the ICT environment in the Department.</p> <p>1.1.4.6 Specifically, how would you setup the Security Operations Centre (SOC) for the Department? Please provide high level architecture and how will you utilise the SOC in managing the overall IT Security environment.</p>																		
<table border="1"> <thead> <tr> <th>Score</th> <th>Meaning</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>○ Non responsive</td> <td>•Not relevant, no evidence / / no information / no inputs</td> </tr> <tr> <td>1</td> <td>○ Poor response</td> <td>• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.</td> </tr> <tr> <td>2</td> <td>○ Good response</td> <td>• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.</td> </tr> <tr> <td>3</td> <td>○ Excellent response</td> <td>•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.</td> </tr> </tbody> </table>				Score	Meaning	Explanation	0	○ Non responsive	•Not relevant, no evidence / / no information / no inputs	1	○ Poor response	• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.	2	○ Good response	• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.	3	○ Excellent response	•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.
Score	Meaning	Explanation																
0	○ Non responsive	•Not relevant, no evidence / / no information / no inputs																
1	○ Poor response	• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.																
2	○ Good response	• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.																
3	○ Excellent response	•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.																
Have you (the bidder) substantiated your response?			<table border="1"> <tr> <td>YES</td> <td>NO</td> </tr> </table>	YES	NO													
YES	NO																	
<table border="1"> <tr> <td> Indicate the corresponding paragraph that specifically substantiates responses in your bid response. </td> <td></td> </tr> </table>				Indicate the corresponding paragraph that specifically substantiates responses in your bid response.														
Indicate the corresponding paragraph that specifically substantiates responses in your bid response.																		

1.1.5	ICT Security Governance, Risk and Compliance Management & Service Delivery Management	15%															
<p>One of the most important requirements for the Department's ICT Security Compliance Management is to secure sensitive information by establishing ICT security processes and complying with the relevant legislation and regulations as it relates to ICT Security. These include, but is not limited to, the following:</p> <ul style="list-style-type: none"> ○ MISS (minimum information security standards) ○ ISO/IEC 27014 (security governance) ○ ISO/IEC 27001 (requirements of an Information Security Management System (ISMS)) ○ ISO/IEC 27005 (risk-based specification of requirements for information security) ○ ISO/IEC 27002 (control framework required to implement an ISMS) <p>Taking into account all the information provided in the specifications, describe:</p> <p>1.1.5.1 how will you meet all requirements of the ICT Security Compliance Management within the stipulated service level standards?</p> <p>1.1.5.2 how will you utilise the specified toolsets to meet all functional requirements of the ICT Security Compliance Management within the stipulated service level standards?</p> <p>1.1.5.3 how will you identify, manage, monitor and report on ICT Security risks?</p> <p>1.1.5.4 how will you ensure compliance with the ISMS control framework?</p> <p>1.1.5.5 how will you effectively utilise the role of ICT Service Delivery Management to meet the RFB requirements?</p>																	
<table border="1"> <thead> <tr> <th>Score</th> <th>Meaning</th> <th>Explanation</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>• Non responsive</td> <td>•Not relevant, no evidence / / no information / no inputs</td> </tr> <tr> <td>1</td> <td>○ Poor response</td> <td>• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.</td> </tr> <tr> <td>2</td> <td>○ Good response</td> <td>• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.</td> </tr> <tr> <td>3</td> <td>○ Excellent response</td> <td>•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.</td> </tr> </tbody> </table>			Score	Meaning	Explanation	0	• Non responsive	•Not relevant, no evidence / / no information / no inputs	1	○ Poor response	• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.	2	○ Good response	• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.	3	○ Excellent response	•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.
Score	Meaning	Explanation															
0	• Non responsive	•Not relevant, no evidence / / no information / no inputs															
1	○ Poor response	• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.															
2	○ Good response	• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.															
3	○ Excellent response	•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.															
Have you (the bidder) substantiated your response?		<table border="1"> <tr> <td>YES</td> <td>NO</td> </tr> </table>	YES	NO													
YES	NO																
<table border="1"> <tr> <td> Indicate the corresponding paragraph that specifically substantiates responses in your bid response. </td> <td></td> </tr> </table>			Indicate the corresponding paragraph that specifically substantiates responses in your bid response.														
Indicate the corresponding paragraph that specifically substantiates responses in your bid response.																	

The manner in which the bidder will perform the Contract Transitioning (Transitioning-In and Transitioning-Out) is considered critical to the Department.

Taking into account requirements for Contract Transitioning (Transitioning-In and Transitioning-Out) services, **and how the Service Towers and their details have been defined and the Contract Positioning Model in this bid**, describe for:

Refer to Annexure C for requirements.

1.1.6.1 Transitioning-In Services:

- 1.1.6.1.1 how will you meet all requirements for Contract Transitioning-In services at the commencement of the contract?
- 1.1.6.1.2 please provide a project plan detailing the activities, the roles and responsibilities (successful bidder, Department and current service provider), and the timeframes to be executed during the Contract Transitioning-In period (one-month period is prescribed).

1.1.6.2 Transitioning-Out Services:

- 1.1.6.2.1 how will you meet all functional requirements for Contract Transitioning-Out services at the end of the contract period?
- 1.1.6.2.2 please provide a project plan detailing the activities, the roles and responsibilities (successful bidder, Department and new service provider), and the timeframes to be executed during the Contract Transitioning-Out period (one-month period is prescribed).

Score	Meaning	Explanation
0	• Non responsive	•Not relevant, no evidence / / no information / no inputs
1	○ Poor response	• Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.
2	○ Good response	• Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.
3	○ Excellent response	•Fully meets and complies with the specification requirements. •Evidence substantiates the requirement. •Additional innovation, best practice standards, benchmark models and better service offerings provided.

Have you (the bidder) substantiated your response?

YES

NO

Indicate the corresponding paragraph that specifically substantiates responses in your bid response.

TOTAL

100

SECTION 6: PRICING SCHEDULES

PRICING SCHEDULE
(Professional Services)

NAME OF BIDDER:.....	BID NO.:
CLOSING TIME 11:00	CLOSING DATE.....

OFFER TO BE VALID FORDAYS FROM THE CLOSING DATE OF BID.

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

1. The accompanying information must be used for the formulation of proposals.
2. Bidders are required to indicate a ceiling price based on the total estimated time for completion of all phases and including all expenses inclusive of all applicable taxes for the project.

R.....
3. PERSONS WHO WILL BE INVOLVED IN THE PROJECT AND RATES APPLICABLE (CERTIFIED INVOICES MUST BE RENDERED IN TERMS HEREOF)
- | 4. PERSON AND POSITION
DAILY RATE | HOURLY | RATE |
|--------------------------------------|--------|------|
| ----- | R----- | ---- |
| ----- | R----- | ---- |
| ----- | R----- | ---- |
| ----- | R----- | ---- |
| ----- | R----- | ---- |
5. PHASES ACCORDING TO WHICH THE PROJECT WILL BE COMPLETED, COST PER PHASE AND MAN-DAYS TO BE SPENT

-----	R-----	days	----
-----	R-----	days	----
-----	R-----	days	----
-----	R-----	days	----

- 5.1 Travel expenses (specify, for example rate/km and total km, class of airtravel, etc). Only actual costs are recoverable. Proof of the expenses incurred must accompany certified invoices.

DESCRIPTION OF EXPENSE TO BE INCURRED	RATE	QUANTITY	AMOUNT
.....	R.....
.....	R.....
.....	R.....
.....	R.....
TOTAL:			R.....

** "all applicable taxes" includes value- added tax, pay as you earn, income tax, unemployment insurance fund contributions and skills development levies.

- 5.2 Other expenses, for example accommodation (specify, eg. Three star hotel, bed and breakfast, telephone cost, reproduction cost, etc.). On basis of these particulars, certified invoices will be checked for correctness. Proof of the expenses must accompany invoices.

DESCRIPTION OF EXPENSE TO BE INCURRED	RATE	QUANTITY	AMOUNT
.....	R.....
.....	R.....
.....	R.....
.....	R.....
TOTAL: R.....			

6. Period required for commencement with project after acceptance of bid

7. Estimated man-days for completion of project

8. Are the rates quoted firm for the full period of contract? *YES/NO

9. If not firm for the full period, provide details of the basis on which adjustments will be applied for, for example consumer price index.

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

Any enquiries regarding bidding procedures may be directed to the – SCM@Justice.gov.za

Service Towers		Cost year 1 (incl. VAT)	Cost year 2 (incl. VAT)	Cost year 3 (incl. VAT)	Total Cost (incl. VAT)
ICT Security Operations Management Services		R	R	R	
ICT Security Monitoring and Reporting Services		R	R	R	
ICT Security Governance, Risk and Compliance, Management Services		R	R	R	
Other Services					
ICT Security Contract - Transition-In and Transition-Out Services	Contract Transition-In			R	
	Contract Transition Out			R	
Other Essential services that the Bidder deems necessary to deliver the services	Other: Specify (monthly)	R	R	R	
	Other Specify (once off – except for the firewalls and proxies) ; proxies or Integrate, Move, and Delete (IMD) R10 million.			R	
GRAND TOTAL		R	R	R	

SECTION 7 - TERMS AND CONDITIONS FOR BIDDING

2. BID SUBMISSION:	
<p>1.1. Bids must be delivered by the stipulated time to the correct address and be deposited inside bid box situated at the Reception (Momentum Building). Late bids will not be considered.</p> <p>1.2. All bids must be submitted on the official forms provided–(not to be re-typed) or online</p> <p>1.3. Bidders must register on the Central Supplier Database (CSDd) to upload mandatory information namely: (Business Registration/ Directorship/ Membership/Identity Numbers; Tax Compliance Status; And Banking Information For Verification Purposes). B-BBEE Certificate or Sworn Affidavit for B-BBEE must be submitted..</p> <p>1.4. Where a bidder is not registered on the CSD, mandatory information namely: (Business Registration/ Directorship/ Membership/Identity Numbers; Tax Compliance status may not be submitted with the bid documentation.</p> <p>1.5. This bid is subject to the General Conditions of Contract (GCC) and, if applicable, any other legislation or special conditions of contract.</p>	
3. TAX COMPLIANCE REQUIREMENTS	
<p>2.1 Bidders must ensure compliance with their tax obligations.</p> <p>2.2 Bidders are required to submit their Unique Personal Identification Number (Pin) issued by SARS to enable the organ of state to view the Taxpayer's Profile and Tax Status.</p> <p>2.3 Application for Tax Compliance Status (TCS) or Pin may also be made via e-Filing. In order to use this provision, taxpayers will need to register with SARS as e-Filers through the website www.sars.gov.za</p> <p>2.4 Bidders may also submit a printed TCS together with the bid.</p> <p>2.5 In bids where Consortia / Joint Ventures / Sub-Contractors are involved, each party must submit a separate proof of TCS / Pin / CSD Number.</p> <p>2.6 Where no TCS is available but the bidder is registered on the Central Supplier Database (CSD), a CSD number must be provided.</p>	
4. QUESTIONNAIRE TO BIDDING FOREIGN SUPPLIERS	
3.1. Is the bidder a resident of the Republic Of South Africa (RSA)?	<input type="checkbox"/> Yes <input type="checkbox"/> No
3.2. Does the bidder have a branch in The RSA?	<input type="checkbox"/> Yes <input type="checkbox"/> No

3.3. Does the bidder have a permanent establishment in the RSA? ☐ Yes ☐ No

3.4. Does the bidder have any source of income in the RSA? ☐ Yes ☐ No

3.5. If the answer is "No" to all of the above, then, it is not a requirement to obtain a Tax Compliance Status / Tax Compliance System Pin Code From The South African Revenue Service (SARS) And If Not Register As Per 2.3 Above.

SECTION 8 - GENERAL CONDITIONS OF CONTRACT (GCC)

GENERAL CONDITIONS OF CONTRACTING (GCC's)

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).

Note: Paragraph 29 relates to Governing language and specifies that the contract shall be written in English. All correspondence and other documents pertaining to the contract that is exchanged by the parties shall also be written in English.

SECTION 9: BIDDING REQUIREMENTS AND SPECIAL BID CONDITIONS

1. DEFINITIONS

- 1.1 "Department" – means the Department of Justice and Constitutional Development.
- 1.2 "DOJ&CD" - means the Department of Justice & Constitutional Development.
- 1.3 "PPPF" – means Preferential Procurement Policy Framework
- 1.4 "RFB" – means Request for Quotation. In this document, RFB and "bid" is used interchangeably and shall have the same meaning and effect.
- 1.5 "Receiving party" – any legal recipient of this document
- 1.6 "Validity Period" – means 120 days commencing from the RFB closing date. This date could be extended by agreement between DOJ&CD and the Bidders.
- 1.7 Business hours- means from 07:30 – 17:00 excluding public holidays and weekends

2. SPECIAL BID CONDITIONS

- 2.1 Confidential Information Disclosure Notice
- 2.2 This document contains confidential information that is the property of the Department of Justice & Constitutional Development (DOJ&CD). This confidentiality clause extends to Bidder partners and/or implementation agents, whom the Bidder may decide to involve in preparing a response to this RFB.
- 2.3 No part of the contents may be used, copied, disclosed or conveyed in whole or in part to any party in any manner whatsoever other than for preparing a proposal in response to this Bid, without prior written permission from the DOJ&CD.
- 2.4 All copyright and Intellectual Property herein vests with DOJ&CD.
- 2.5 For purposes of this process, the term "Confidential Information" shall include all technical and business information, including, without limiting the generality of the foregoing, all secret knowledge and information (including any and all financial, commercial, market, technical, functional and scientific information, and information relating to a party's strategic objectives and planning and its past, present and future research and development), technical, functional and scientific requirements and specifications, data concerning business

relationships, demonstrations, processes, machinery, know-how, architectural information, information contained in a party's software and associated material and documentation,

- 2.6 Plans, designs and drawings and all material of whatever description, whether subject to or protected by copyright, patent or trademark, registered or un-registered, or otherwise disclosed or communicated before or after the date of this process.
- 2.7 The receiving party shall not, during the period of validity of this process, or at any time thereafter, use or disclose, directly or indirectly, the confidential information of DOJ&CD (even if received before the date of this process) to any person whether in the employment of the receiving party or not, who does not take part in the performance of this process.
- 2.8 The receiving party shall take all such steps as may be reasonably necessary to prevent DOJ&CD's confidential information coming into the possession of unauthorised third parties. In protecting the receiving party's confidential information, DOJ&CD shall use the same degree of care, which does not amount to less than a reasonable degree of care, to prevent the unauthorised use or disclosure of the confidential information as the receiving party uses to protect its own confidential information.
- 2.9 The DOJ&CD shall reserve the right to, prior to the awarding of the tender, enter into price negotiation with the preferred tenderer(s).
- 2.10 Any documentation, software or records relating to confidential information of DOJ&CD, which comes into the possession of the receiving party during the period of validity of this process or at any time thereafter or which has so come into its possession before the period of validity of this process:
 - 2.10.1 Shall be deemed to form part of the confidential information of DOJ&CD;
 - 2.10.2 Shall be deemed to be the property of DOJ&CD;
 - 2.10.3 Shall not be copied, reproduced, published or circulated by the receiving party unless and to the extent that such copying is necessary for the performance of this process and all other processes as contemplated in; and

- 2.10.4 Shall be surrendered to DOJ&CD on demand, and in any event on the termination of the investigations and negotiations, and the receiving party shall not retain any extracts.

3. BID / RFB SPECIFICATIONS – LEGAL REVIEW

- 3.1 Any bidder who has reasons to believe that any clause of this specification is in conflict with any applicable legislation in the Republic of South Africa, must inform the Department in writing, stating reasons for believing such (quoting applicable legislation & clauses), before the clarification questions closing date.

4. NEWS AND PRESS RELEASES

- 4.1 Bidders or their agents shall not make any news releases concerning this RFB or the awarding of the same or any resulting agreement(s) without the consent of, and then only in co-ordination with DOJ&CD.

5. PRECEDENCE OF DOCUMENTS

- 5.1 This RFB consists of a number of sections. Where there is a contradiction in terms between the clauses, phrases, words, stipulations or terms and herein referred to generally as stipulations in this RFB and the stipulations in any other document attached hereto, or the RFB submitted hereto, the relevant stipulations in this RFB shall take precedence.
- 5.2 Where this RFB is silent on any matter, the relevant stipulations addressing such matter and which appear in the PPPFA shall take precedence. Bidders shall refrain from incorporating any additional stipulations in its proposal submitted in terms hereof other than in the form of a clearly marked recommendation that DOJ&CD may in its sole discretion elect to import or to ignore. Any such inclusion shall not be used for any purpose of interpretation unless it has been so imported or acknowledged by DOJ&CD.
- 5.3 It is acknowledged that all stipulations in the PPPFA are not equally applicable to all matters addressed in this RFB. It however remains the exclusive domain and election of DOJ&CD as to which of these stipulations are applicable and to what extent. Bidders are hereby acknowledging that the decision of DOJ&CD in this regard is final and binding. The onus to enquire and obtain clarity in this regard rests with the Bidder(s). The Bidder(s) shall take care to restrict its enquiries in this regard to the most reasonable interpretations required to ensure the necessary consensus.

6. BIDDER QUERIES

- 6.1 Should it be necessary for a bidder to obtain clarity on any matter arising from or referred to in this RFB document, please refer queries, in writing to the e-mail address below. Please ensure that the RFB number is stipulated in the subject line of your e-mail.

E-mail address
<u>SCM@justice.gov.za</u>

- 6.2 Under no circumstances may any other employee within DOJ&CD, other than the contact person provided above, be approached for any information. Any such action may result in a disqualification of a response submitted in competition to the RFB.
- 6.3 DOJ&CD reserves the right to place a received query and it's corresponding response thereto, on its website, or a website that it has officially selected for such correspondence.
- 6.4 Any bidder who has reasons to believe that this specification is written in such a manner that it favours any organization, must inform the Department in writing, stating reasons for believing such, before the clarification questions closing date.
- 6.5 Language: All correspondence for this bid shall be in English.

SECTION 10 - ANNEXURES

Annexure A - Overall Bidder Experience

[illegible]

Annexure B - Bidder Human Resources Experience (only complete for onsite resources on a full-time basis)

Primary Human Resource Requirements			Critical Human Resource Profile			Project Profile	
Service Tower	Resources	Qty	Name of Resource(s)	Resource(s) Qualifications (max 3)	Resource(s) Experience (min 3 years)	Name of organisation(s) where projects were implemented (max 5)	Name of projects implemented (max 5)
Security Operations Management	Firewall Engineer	1					
	Internet Security Specialist	1					
	Junior Internet Security Engineer	1					
	Trend Micro Senior Specialist	1					
	Security Engineers	2					
IT Security Monitoring and Reporting	Senior IT Security Monitoring Analyst	1					
	Junior IT Security Monitoring Analyst	1					
	Senior IT Security Governance Compliance & Risk Manager	1					

Annexure B¹ - Bidder Human Resources Experience (only complete for onsite resources on a full-time basis)

Service Tower	Title	Qty	Certificates
Security Operations Management	Firewall Engineer	1	<ul style="list-style-type: none"> • Checkpoint Certification; or • Certified Information Systems Security Professional Certification; or • CompTIA Security+
	Internet Security Specialist	1	<ul style="list-style-type: none"> • Certified Information Systems Security Professional Certification; or • CompTIA Security+ • Certified Ethical Hacker (CEH)
	Junior Internet Security Engineer	1	<ul style="list-style-type: none"> • Certified Information Systems Security Professional Certification; or • CompTIA Security+ • Certified Ethical Hacker (CEH)
	Trend Micro Senior Specialist	1	<ul style="list-style-type: none"> • Trend products Certification • CompTIA Advanced Security Practitioner Certificate+

Service Tower	Title	Qty	Certificates
	Security Engineers	2	<ul style="list-style-type: none"> • Certified Information Systems Security Professional Certification; or • CompTIA Security+; or • Certified Ethical Hacker (CEH); or • Certified Information Security Manager Certification; or
	Cloud Email Engineer	1	<ul style="list-style-type: none"> • CompTIA Security+ Certificate; or • MIMECAS • Certification; or • Certificate of Cloud Security Knowledge (CCSK)
IT Security Monitoring and Reporting	Senior IT Security Monitoring Analyst	1	<ul style="list-style-type: none"> • GIAC Security Essentials Certification • Certified Information Systems Security Professional Certification; or • CompTIA Security+; or • Security Information and Event Management Certificate

Score	Meaning	Explanation
0	○ Non responsive	<ul style="list-style-type: none"> • Not relevant, no evidence / no information / no inputs
1	○ Poor response	<ul style="list-style-type: none"> • Meets some, but not all of the minimum requirements. • Evidence not enough to substantiate the requirement.
2	○ Good response	<ul style="list-style-type: none"> • Fully meets and complies with the specification requirements. • Evidence substantiates the requirements.
3	○ Excellent response	<ul style="list-style-type: none"> • Fully meets and complies with the specification requirements. • Evidence substantiates the requirement. • Additional innovation, best practice standards, benchmark models and better service offerings provided.

ANNEXURE C TRANSITION-IN / OUT REQUIREMENTS

PURPOSE

This requirement formally documents the process for the transition of the responsibilities, duties, activities, and functions for the services to be rendered during the contract period. The transition-in period will commence as from issuing letter of award to the winning bidder and upon the date as stipulated.

TRANSITION APPROACH

For this transition-in period, the New Contractor shall maintain its staff on-site throughout the initial transition period of one month. No additional staffing requirements are anticipated to complete the transition. Immediately prior to the transition, the Incumbent Contractor shall set up its transition team in order to facilitate the activities necessary for successful transition. The New Contractor will have its staff on site the first day of the transition period and will establish a team to coordinate the contract transition. The department will provide adequate workspace for both contractors throughout the duration of the transition. The department will also designate a Transition Manager to work with both Contractors throughout the transition period.

TRANSITION TEAM ORGANIZATION

The following table illustrates the transition team members from the department, Incumbent Contractor, and the new Contractor as well as the roles and responsibilities of each team member.

Organization	Title	Name	Roles/Responsibilities
DOJ&CD	Transition Manager	TBC	Coordinate activities between contractors throughout transition; provide workspace for all transition staff; facilitate transition meetings as required.

DOJ&CD	Contract Manager	TBC	Responsible for overseeing all contract actions and deliverables; responsible and for ensuring accountability.
Incumbent Contractor	Transition Lead	TBC	Work with the department and Contractor managers and leads to coordinate and schedule all transition activities; provide weekly reporting on transition progress; ensure all applicable property and tools are included as part of transition.
Incumbent Contractor	Transition Manager	TBC	Ensure all activities are completed during transition; document all processes, tasks, and activities for transition to Future Contractor; ensure all training documentation is complete; ensure completion of user and technical manuals and processes; ensure all documentation is in accordance with the department's standards; ensure proprietary materials are not part of transition.
New Contractor	Transition Lead	TBC	Work with the department and Incumbent Contractor managers and leads; ensure all transition deliverables are received and understood; identify any gaps in transition activities
New Contractor	Transition Manager	TBC	Ensure continuity of all activities throughout transition; ensure receipt of adequate documentation of all processes, tasks, and

			activities; ensure all training documentation addresses all planned training items; ensure standardization of all transitioned documentation
DOJ&CD	Transition Manager	TBC	Coordinate activities between contractors throughout transition; provide workspace for all transition staff; facilitate transition meetings as required.

WORKFORCE TRANSITION

For this transition, all workforce members shall remain with their current organization. The Incumbent Contractor workforce shall remain on-site to perform their transition activities until such time that the transition is completed and approved by all parties. The new contractor shall ensure its workforce is on site until transition completion. This will allow adequate time to perform all transition activities. The department will provide any additional temporary workspace needed for the new Contractor employees until transition completion, at which time the workforce will occupy the vacated locations of the outgoing Incumbent Contractor workforce.

WORK EXECUTION DURING TRANSITION

Throughout the transition phase, work shall continue to be performed by Incumbent Contractor in accordance with the current contract. The transition management team shall ensure that the new Contractor's employees work alongside Incumbent Contractor counterparts; however, Incumbent Contractor shall maintain all responsibility for tasks and deliverables. At the end of the transition period or the award of the new contract with the new Contractor (whichever happens first), and upon transition approval, the new Contractor shall assume full responsibility for all tasks and deliverables.

PROPERTY TRANSITION

DOJ&CD Furnished Property and Controls

As part of this transition, all furnished property provided by the department to the Incumbent Contractor under the current services contract shall be turned in to the department upon completion and approval of the transition phase. This includes all facility and access keys, ID badges, tools, equipment, and controls. A listing of furnished property, equipment and tools will be provided upon commencement of the transition process.

Incumbent Contractor Owned Property

All incumbent owned equipment shall remain with Incumbent Contractor upon completion and approval of the transition.

KNOWLEDGE TRANSFER

For this transition, knowledge transfer shall occur over the entirety of the 30 day transition period. The knowledge transfer shall take place via various methods. Incumbent Contractor's Transition Manager shall coordinate transition sessions that focus on the specific functionality, activities, and concerns related to the department's reuse services and operations management. These sessions shall be completed no later than 60 calendar days prior to the end of the transition period. Additionally, the new Contractor's staff will work alongside their Incumbent Contractor counterparts throughout the 30 day period in order to gain familiarity with the equipment, software, tools, processes, and organizational assets. The Transition Managers from Incumbent Contractor, the new Contractor, and the department shall meet no later than 30 calendar days prior to transition completion in order to determine if any further training or knowledge transfer is required.

SCHEDULE

The Incumbent Contractor's Transition Manager shall develop a schedule and associated tasks for transitioning all services under their contract to the new Contractor. The schedule with outlined further tasks to be completed and any changes to this schedule will require review and approval from the departments Transition Manager.

HANDOVER AND ACCEPTANCE

The department will make the determination of when transition is completed and will provide formal acceptance indicating such. To do this, the department's Transition Manager will utilize the established transition checklist in below in order to determine that all activities associated with the transition have been completed. The department's Transition Manager will also meet with or contact the Transition Managers from Incumbent Contractor and the new Contractor to ensure that all concerns and issues have been met and addressed appropriately. Once the department's Transition Manager has formally accepted the transition as complete, the checklist and supporting documentation will be signed and accepted by the department's Transition Manager and will be sent to the department's Supply Chain Management to upload to the current contract file. It is only after all of these approvals and signatures are in place that the transition will be considered complete.

DOJ&CD / NEW CONTRACTOR TRANSITION-IN CHECKLIST AND ACTIVITIES

CHECKLIST COMMENTS/NOTES

Completed Y/N	Checklist	Comments / Notes
	Organise a start-up meeting with the incoming supplier	

	Prepare a timeline of activities/events and obtain a copy of the incoming supplier's transition in plan – where relevant	
	Confirm the transition in obligations (including roles and responsibilities, timeframes and resources) set out in the contract	
	Note the specific differences between the previous contract and the new contract - where relevant (e.g. changes in scope, delivery, timeframes, policies/procedures, and the contract terms and conditions)	
	Develop other plans if required e.g. Risk Management Plan, Communication Plan, Stakeholder Engagement Plan, Probity Plan, Disposal Plan.	
	Establish contract administration procedures and access to policies, procedures and other instructions	
	Arrange access to facilities, equipment, assets, systems etc. (including user accounts and other authorisations)	
	Record/Confirm the new supplier's vendor details	
	Facilitate the transfer / handover of clients and client records from outgoing supplier – where relevant	
	Conduct staff training – if contract is new or significantly different, or if supply arrangements will change	
	Establish a communication strategy for purchasing under the new contract – where relevant	
	Manage the transfer of intellectual property during the transition period	

**DOJ&CD / NEW CONTRACTOR / INCUMBENT CONTRACT TRANSITION-IN / OUT
CHECKLIST AND ACTIVITIES**

CHECKLIST COMMENTS/NOTES

Completed Y/N	Checklist	Comments / Notes
	Confirm the transition out obligations (including roles and responsibilities, timeframes and resources) set out in the contract	
	Prepare a timeline of activities/events and obtain a copy of the outgoing supplier's transition out plan – where relevant	
	Review the Risk Management Plan, Communication Plan, Stakeholder Engagement Plan and Disposal Plan and undertake any actions	
	Retrieve any relevant documents, reports or information from outgoing supplier	
	Confirm that all access cards/security badges used by service providers, contractors or suppliers are returned	
	Deactivate systems etc. (including user accounts, passwords and other authorisations)	
	Organise return of any equipment and assets	
	Confirm that disposal obligations are fulfilled	
	Facilitate the transfer / handover of clients and client records to the incoming supplier – where relevant	

	Ensure client records are closed or stored confidentially and accurately – where relevant	
	Rectify any supplier contractual defects and non-conformances	
	Issue handover/acceptance certification/s where relevant	
	Document and confirm date of the close-out of all claims (insurance, warranties, guarantees and licensing)	
	Finalise and archive contracts and relevant documents	
	Review and record any post transition in findings	

TRANSITION COMPLETE & APPROVED BY:

DOJ&CD Transition Manager

Name: Date:

Signature:

DOJ&CD Director Infrastructure Operations

Name: Date:

Signature:

ANNEXURE D: INVITATION TO BID**SBD 1**

YOU ARE HEREBY INVITED TO BID FOR REQUIREMENTS OF THE DEPARTMENT OF JUSTICE & CONSTITUTIONAL DEVELOPMENT				
BID NUMBER:	RFQ 07 2022	CLOSING DATE:	07 November 2022 @ 11:00 AM	
DESCRIPTION	APPOINTMENT OF A SERVICE PROVIDER FOR INFORMATION COMMUNICATION TECHNOLOGY (ICT) SECURITY SUPPORT SERVICES FOR A PERIOD OF 3 YEARS(INCLUSIVE OF ONE MONTH TRANSITIONING-IN AND ONE MONTH TRANSITIONING-OUT SERVICES WITHIN THE CONTRACT PERIOD)			
BID RESPONSE DOCUMENTS MUST BE DEPOSITED IN THE TENDER / BID BOX SITUATED ATDOJ&CD, MOMENTUM BUILDING, 329 PRETORIUS STREET, C/O SISULU & PRETORIUS STREET, PRETORIA, 0001				
SUPPLIER INFORMATION				
NAME OF BIDDER				
POSTAL ADDRESS				
STREET ADDRESS				
TELEPHONE NUMBER	CODE		NUMBER	
CELLPHONE NUMBER				
FACSIMILE NUMBER	CODE		NUMBER	
E-MAIL ADDRESS				
VAT REGISTRATION NUMBER				
	TCS PIN:		OR	CSD No:
B-BBEE STATUS LEVEL VERIFICATION	<input type="checkbox"/> Yes <input type="checkbox"/> No		B-BBEE STATUS LEVEL	<input type="checkbox"/> Yes <input type="checkbox"/> No

CERTIFICATE [TICK APPLICABLE BOX]		SWORN AFFIDAVIT	
IF YES, WHO WAS THE CERTIFICATE ISSUED BY?			
AN ACCOUNTING OFFICER AS CONTEMPLATED IN THE CLOSE CORPORATION ACT (CCA) AND NAME THE APPLICABLE IN THE TICK BOX	<input type="checkbox"/>	AN ACCOUNTING OFFICER AS CONTEMPLATED IN THE CLOSE CORPORATION ACT (CCA)	
	<input type="checkbox"/>	A VERIFICATION AGENCY ACCREDITED BY THE SOUTH AFRICAN ACCREDITATION SYSTEM (SANAS)	
	<input type="checkbox"/>	A REGISTERED AUDITOR	
		NAME:	
[A B-BBEE STATUS LEVEL VERIFICATION CERTIFICATE/SWORN AFFIDAVIT(FOR EMEs& QSEs) MUST BE SUBMITTED IN ORDER TO QUALIFY FOR PREFERENCE POINTS FOR B-BBEE]			
ARE YOU THE ACCREDITED REPRESENTATIVE IN SOUTH AFRICA FOR THE GOODS /SERVICES /WORKS OFFERED?	<input type="checkbox"/> Yes <input type="checkbox"/> No [IF YES ENCLOSE PROOF]	ARE YOU A FOREIGN BASED SUPPLIER FOR THE GOODS /SERVICES /WORKS OFFERED?	<input type="checkbox"/> Yes <input type="checkbox"/> No [if yes answer part b:3 below]
SIGNATURE OF BIDDER	DATE	
CAPACITY UNDER WHICH THIS BID IS SIGNED			
TOTAL NUMBER OF ITEMS OFFERED		TOTAL BID PRICE (ALL INCLUSIVE)	

BIDDING PROCEDURE ENQUIRIES MAY BE DIRECTED TO:		TECHNICAL INFORMATION MAY BE DIRECTED TO:	
DEPARTMENT/ PUBLIC ENTITY	DEPARTMENT OF JUSTICE & CONSTITUTIONAL DEVELOPMENT		
CONTACT PERSON	E-Mail all bidding procedure enquiries to <u>SCM@justice.gov.za</u>	CONTACT PERSON	E-Mail all technical information enquiries to <u>SCM@justice.gov.za</u>
TELEPHONE NUMBER		TELEPHONE NUMBER	
FACSIMILE NUMBER		FACSIMILE NUMBER	
E-MAIL ADDRESS		E-MAIL ADDRESS	

BIDDER'S DISCLOSURE**1. PURPOSE OF THE FORM**

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

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

2. Bidder's declaration

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

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

Full Name	Identity Number	Name of State institution

- 2.2 Do you, or any person connected with the bidder, have a relationship with any person who is employed by the procuring institution? **YES/NO**

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

2.2.1

If so, furnish particulars:

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

2.3.1 If so, furnish particulars:

3 DECLARATION

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

- 3.1 I have read and I understand the contents of this disclosure;
- 3.2 I understand that the accompanying bid will be disqualified if this disclosure is found not to be true and complete in every respect;
- 3.3 The bidder has arrived at the accompanying bid independently from, and without consultation, communication, agreement or arrangement with any competitor. However, communication between partners in a joint venture or consortium² will not be construed as collusive bidding.
- 3.4 In addition, there have been no consultations, communications, agreements or arrangements with any competitor regarding the quality, quantity, specifications, prices, including methods, factors or formulas used to calculate prices, market allocation, the intention or decision to submit or not to submit the bid, bidding with the intention not to win the bid and conditions or delivery particulars of the products or services to which this bid invitation relates.
- 3.4 The terms of the accompanying bid have not been, and will not be, disclosed by the bidder, directly or indirectly, to any competitor, prior to the date and time of the official bid opening or of the awarding of the contract.
- 3.5 There have been no consultations, communications, agreements or arrangements made by the bidder with any official of the procuring institution in relation to this procurement process prior to and during the bidding process except to provide clarification on the bid submitted where so required by the institution; and the bidder was not involved in the drafting of the specifications or terms of reference for this bid.
- 3.6 I am aware that, in addition and without prejudice to any other remedy provided to combat any restrictive practices related to bids and contracts, bids that are suspicious will be reported to the Competition Commission for investigation and possible imposition of administrative penalties in terms of section 59 of the Competition Act No 89 of 1998 and or may be reported to the National Prosecuting Authority (NPA) for criminal investigation and or may be restricted from conducting business with the public sector for a period not exceeding ten (10) years in terms of the Prevention and Combating of Corrupt Activities Act No 12 of 2004 or any other applicable legislation.

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

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

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

.....
Signature

.....
Date

.....
Position

.....
Name of bidder

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

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

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

1. GENERAL CONDITIONS

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

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2

- a) The value of this bid is estimated to exceed/not exceed R50 000 000 (all applicable taxes included) and therefore the ...**80/20**..... preference point system shall be applicable; or
- b) Either the 80/20 or 90/10 preference point system will be applicable to this tender (*delete whichever is not applicable for this tender*).

1.3 Points for this bid shall be awarded for:

- (a) Price; and
- (b) B-BBEE Status Level of Contributor.

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

	POINTS
PRICE	80
B-BBEE STATUS LEVEL OF CONTRIBUTOR	20
Total points for Price and B-BBEE must not exceed	100

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

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

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

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

1. GENERAL CONDITIONS

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

- the 80/20 system for requirements with a Rand value of up to R50 000 000 (all applicable taxes included); and
- the 90/10 system for requirements with a Rand value above R50 000 000 (all applicable taxes included).

1.2

- a) The value of this bid is estimated to exceed/not exceed R50 000 000 (all applicable taxes included) and therefore the ...**80/20**..... preference point system shall be applicable; or
- b) Either the 80/20 or 90/10 preference point system will be applicable to this tender (*delete whichever is not applicable for this tender*).

1.3 Points for this bid shall be awarded for:

- (a) Price; and
- (b) B-BBEE Status Level of Contributor.

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

	POINTS
PRICE	80
B-BBEE STATUS LEVEL OF CONTRIBUTOR	20
Total points for Price and B-BBEE must not exceed	100

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

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

2. DEFINITIONS

- (a) **“B-BBEE”** means broad-based black economic empowerment as defined in section 1 of the Broad-Based Black Economic Empowerment Act;
- (b) **“B-BBEE status level of contributor”** means the B-BBEE status of an entity in terms of a code of good practice on black economic empowerment, issued in terms of section 9(1) of the Broad-Based Black Economic Empowerment Act;

- (c) **“bid”** means a written offer in a prescribed or stipulated form in response to an invitation by an organ of state for the provision of goods or services, through price quotations, advertised competitive bidding processes or proposals;
- (d) **“Broad-Based Black Economic Empowerment Act”** means the Broad-Based Black Economic Empowerment Act, 2003 (Act No. 53 of 2003);
- (e) **“EME”** means an Exempted Micro Enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;
- (f) **“functionality”** means the ability of a tenderer to provide goods or services in accordance with specifications as set out in the tender documents.
- (g) **“prices”** includes all applicable taxes less all unconditional discounts;
- (h) **“proof of B-BBEE status level of contributor”** means:
 - 1) B-BBEE Status level certificate issued by an authorized body or person;
 - 2) A sworn affidavit as prescribed by the B-BBEE Codes of Good Practice;
 - 3) Any other requirement prescribed in terms of the B-BBEE Act;
- (i) **“QSE”** means a qualifying small business enterprise in terms of a code of good practice on black economic empowerment issued in terms of section 9 (1) of the Broad-Based Black Economic Empowerment Act;
- (j) **“rand value”** means the total estimated value of a contract in Rand, calculated at the time of bid invitation, and includes all applicable taxes;

3. POINTS AWARDED FOR PRICE

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

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

80/20

or

90/10

$$P_s = 80 \left(1 - \frac{P_t - P_{\min}}{P_{\min}} \right) \quad \text{or} \quad P_s = 90 \left(1 - \frac{P_t - P_{\min}}{P_{\min}} \right)$$

Where

P_s = Points scored for price of bid under consideration

P_t = Price of bid under consideration

P_{\min} = Price of lowest acceptable bid

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

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

B-BBEE Status Level of Contributor	Number of points (90/10 system)	Number of points (80/20 system)
------------------------------------	---------------------------------	---------------------------------

1	10	20
2	9	18
3	6	14
4	5	12
5	4	8
6	3	6
7	2	4
8	1	2
Non-compliant contributor	0	0

5. BID DECLARATION

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

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

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

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

7. SUB-CONTRACTING

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

(*Tick applicable box*)

YES	<input type="checkbox"/>	NO	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

- 7.1.1 If yes, indicate:

- What percentage of the contract will be subcontracted.....%
- The name of the sub-contractor.....
- The B-BBEE status level of the sub-contractor.....
- Whether the sub-contractor is an EME or QSE

(*Tick applicable box*)

YES	<input type="checkbox"/>	NO	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

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

Designated Group: An EME or QSE which is at last 51% owned by:	EME	QSE
	✓	✓

Black people		
Black people who are youth		
Black people who are women		
Black people with disabilities		
Black people living in rural or underdeveloped areas or townships		
Cooperative owned by black people		
Black people who are military veterans		
OR		
Any EME		
Any QSE		

8. DECLARATION WITH REGARD TO COMPANY/FIRM

8.1 Name _____ of
company/firm:.....

8.2 VAT _____ registration
number:.....

8.3 Company _____ registration
number:.....

8.4 TYPE OF COMPANY/ FIRM

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

[TICK APPLICABLE BOX]

8.5 DESCRIBE PRINCIPAL BUSINESS ACTIVITIES

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

8.6 COMPANY CLASSIFICATION

- ☐ Manufacturer
- ☐ Supplier
- ☐ Professional service provider

☐ Other service providers, e.g. transporter, etc.
[TICK APPLICABLE BOX]

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

8.8 I/we, the undersigned, who is / are duly authorised to do so on behalf of the company/firm, certify that the points claimed, based on the B-BBE status level of contributor indicated in paragraphs 1.4 and 6.1 of the foregoing certificate, qualifies the company/ firm for the preference(s) shown and I / we acknowledge that:

- i) The information furnished is true and correct;
- ii) The preference points claimed are in accordance with the General Conditions as indicated in paragraph 1 of this form;
- iii) In the event of a contract being awarded as a result of points claimed as shown in paragraphs 1.4 and 6.1, the contractor may be required to furnish documentary proof to the satisfaction of the purchaser that the claims are correct;
- iv) If the B-BBEE status level of contributor has been claimed or obtained on a fraudulent basis or any of the conditions of contract have not been fulfilled, the purchaser may, in addition to any other remedy it may have –
 - (a) disqualify the person from the bidding process;
 - (b) recover costs, losses or damages it has incurred or suffered as a result of that person's conduct;
 - (c) cancel the contract and claim any damages which it has suffered as a result of having to make less favourable arrangements due to such cancellation;
 - (d) recommend that the bidder or contractor, its shareholders and directors, or only the shareholders and directors who acted on a fraudulent basis, be restricted by the National Treasury from obtaining business from any organ of state for a period not exceeding 10 years, after the *audi alteram partem* (hear the other side) rule has been applied; and
 - (e) forward the matter for criminal prosecution.

WITNESSES

- 1.
- 2.

.....
SIGNATURE(S) OF BIDDERS(S)

DATE:

ADDRESS