Compulsory Briefing Session Minutes for the appointment of a service provider to perform a cybersecurity risk assessment and to develop and IT security strategy for the National Development Agency (NDA) within a period of three (03) months
19 October 2022
Microsoft Teams
Time: 10h00

Attendees: Ms Lerato Dhlamini – BSC Member
Mr Thabang Moloi – BSC Member
Dr Nthabiseng Kraai – BSC Member
Mr Muzi Matsenjwa – BSC Member
Mr Lunga Mbatha – BSC Member/Secretariat
Service providers

NO.	ITEM	RESPONSIBLE	ATTACHMENTS
1.	**PROCEDURAL MATTERS**		
1.1	**Opening and Welcome** Mr Muzi Matsenjwa opened the meeting, welcomed everybody connected and explained the purpose of the meeting.	**Chairperson**	
2.	**DISCUSSIONS**		
2.1	Mr Muzi Matsenjwa went through the commercial requirements of the TORs and highlighted the following: ▪ Closing date and time for tender submission is 31October 2022 at 12:00. ▪ Minutes to be emailed and published within 5 Days of the briefing ▪ A two-envelope system will be used for commercial and technical requirements ▪ Mandatory documents in Section 17 of the TORs. ▪ Only service providers who joined the compulsory briefing session will be eligible for submitting bids. ▪ Mandatory documents not submitted will lead to disqualification. ▪ Mr Matsenjwa emphasized the importance of including all required mandatory documents. ▪ All SBD documents must be fully completed, dated, and signed. ▪ Bidders must make sure that a letter of authority is signed on the bidder's letterhead and submitted in the commercial envelope. ▪ Bidders must capture their contact details (contact number and email address) and company names on the chat box as proof that they attended the compulsory briefing session.	**All**	
2.2			

NO.	ITEM	RESPONSIBLE	ATTACHMENTS
	Ms Lerato Dhlamini went through the technical evaluation of the TORs and highlighted the following: - • The Scope of work as per section 4 of the TORs • Deliverables • Technical Evaluation Criteria.		
3.	**CLOSURE**		
	Meeting adjourned at 11:40pm		

QUESTIONS & ANSWERS	
Questions from Service Providers	**Responses from NDA**
One scanning component may not be enough to review the gaps in information. Their rule of thumb is they do two over a period, in the 3 months is NDA looking for one full assessment to be done?	The NDA requires a full assessment, for the gaps to be identified and a strategy to be documented. Assessment of all tests, from technical to soft issues with recommendations.
When will the tender be awarded?	The tender should be awarded by the end of November 2022.
After the advisory service has been given as per the tender, will there be another RFP on how gaps should be fixed or is it part of this tender?	The implementation plans will serve as guide to the approach; however the actual implementation of the security strategy will follow a different procurement process.
Will the service provider who is awarded this tender be excluded from future RFP for implementation?	The merits and demerits and possible conflict of interests will be evaluated at a later stage. All service providers that have the capacity to submit proposals are encouraged to do so without fear that they may be excluded to implement the project.
How many firewalls and ports are to be scanned?	There are 10 active firewalls, and all ports must be scanned.
From the scope point of view, is the penetration testing only limited to the internal or external environment, if not how many hosts are external facing, how many wireless access points does the NDA have, what is the total number of web	Both internal and external, the NDA requires a 360-degree assessment. The NDA ICT team will respond in writing and confirm.

QUESTIONS & ANSWERS	
Questions from Service Providers	**Responses from NDA**
application in scope of the projects and How many ICT security policies and procedures need to be revised?	The NDA has one ICT security policy and 3-5 related SOPs to be considered. The bidder will recommend based on the assessment.
Can bidders, bid for part of the tender?	No, they cannot as the submission will be incomplete. Bidders can consider a joint venture submission.
Would the NDA prefer a white, grey, and black testing for everything in scope?	Yes, refer to 4.1.2 of the scope.
Do web applications offer any transactional services?	Yes, the web application is transactional
Should Certificates be certified and how long should the certification be valid for?	Between one and 3 years
Does the NDA require a higher-level strategic component included, such as vision, principles, swot analysis, crown analysis?	The bidders will guide the NDA, they must be inclusive in developing a strategy in terms of areas to be addressed.
It is indicated that the NDA has 200 employees, the assumption is that there 200 workstations, are the employees working centrally or are they remotely?	The NDA is a hybrid environment, employees work both centrally and remotely.
Where are the NDA's central data centre located, physically?	The data centre is located at Head Office in Johannesburg.
How do the branches connect to the data centre, is it through an internal network, MPLS or LTE?	They connect with MPLS and LTE network connection.
Is the disaster recovery site included in the scope of work?	Yes, it is included.
Will the 3rd party risk be in scope with the assessment?	The 3rd party assessment will be linked to the rendering of services to the NDA, or web application that are hosted at

QUESTIONS & ANSWERS	
Questions from Service Providers	**Responses from NDA**
	their data centre to assess the risk in term of the agreement, but not necessarily to do a risk assessment on them.
Will the existing strategy and framework be shared with bidders to review and modernise?	Yes, they will be provided to the service provider, post contracting.
Does the NDA have a list of 3rd party service providers and the service the NDA consume from them?	To be provided post contracting
A follow up in terms of the time frame, does the NDA believe three months is a reasonable time frame?	As per the scope, 3 months is a reasonable time frame, as the NDA has done this exercise before.
Taking into consideration the regulatory/legislative review such as cyber security act to cover the data governance, that inform the question around the 3 months' time frame. Is the legislative review part of the ad hoc work, as there wasn't much provision for it in the TORs, will it be one of the things that bidders can motivate for more time frame?	Yes, bidders can motivate. Bidders should assess their own resources, reviewing of policies should not necessarily depend on any technical assessment. Service providers can have their team running activities parallel, and if the NDA says they would like to review policies to ensure they comply with regulation. Some of the activities are not reliant on the NDA's availability, it is the work that the service provider can do in the background if they have adequate expertise.
The NDA is asking for ad hoc services which are 15% of the contract value, what is the scope of these ad hoc services as opposed to a follow up tender to do a full remedial project once the assessment has been done and completed?	The 15% ad hoc services are standard with the NDA ICT tenders, to make provision for value-add implementations, which the NDA did not consider and can be executed within the project without going out on another RFP.
If the bidder does not have reference letters from their current client due to non-disclosure agreements, will the NDA be able to contact these service providers to confirm referrals?	For NDA to contact the clients would mean a bidder has already disclosed, Bidder must approach clients and notify them that they are bidding for a similar project. The client can confirm that they are providing similar service, without disclosing sensitive information, but just to indicate the scope. In that case, they have not breached the non-

QUESTIONS & ANSWERS	
Questions from Service Providers	**Responses from NDA**
	disclosure. They don't need to give details of the solutions implemented, just the scope.
Is the test related to a compliance / regulation requirement?	Yes. ISO 27001, Cybercrime act, POPIA
When can the penetration test be conducted?	It will depend on the project planning post contracting.
How many internal IPs are being tested?	300
How many external IPs are being tested?	10 Plus
If internal penetration testing is required, is remote access going to be provided to the penetration tester to do necessary work for internal IPs testing? Or pen tester must be onsite?	Bidders should consider the type of testing required (White, Grey and Black)
The count of IPs in scope	5
Are there any security devices in place that could affect our testing (i.e., FW, IDS / IPS, WAF, and Load Balancer)?	It does not matter, the aim is to breach any security controls.
What type of testing are you expecting?	As per the TOR
Is web application penetration test required as part of the penetration testing?	Yes
How many web applications are in the scope of testing?	12
Are the applications hosted on the cloud or your premises?	Hybrid (Both)
How many login systems are being assessed?	2
How many static pages are being assessed (approximate)?	N/A
How many dynamic pages are being assessed (approximate)?	To be confirmed post contracting
Will the web app source code be made readily available?	N/A
Will static analysis be performed?	Yes
Do you require role-based testing against the application?	Yes

QUESTIONS & ANSWERS	
Questions from Service Providers	**Responses from NDA**
Do you require credentialed scans of web apps?	Yes
Is mobile application penetration test required as part of the penetration testing?	Yes
How many mobile applications are in the scope of testing?	3
Platform of App, is it Android or IOS	Both
Is wireless network penetration test required as part of the penetration testing?	Yes
How many networks are in place?	APN, MPLS, LTE
How many active sites and how many active configurations of wireless devices exist?	9
Is a guest wireless network used?	Yes
Is configuration review also part of scope?	Yes
Does the guest network require authentication?	Yes
What type of encryption is used on the wireless network?	Bidder to recommend
What is the square footage of the wireless coverage?	Unknown
Is Phishing Simulation campaign required as part of the penetration testing?	Yes
If yes, does the client have a list of email addresses they would like a phishing Simulation to be performed against?	To be confirmed post contracting
How many mailboxes are in place?	220
what is the frequency of the campaigns (for example twice per year)	Bidder to recommend
Is vulnerability assessment required as part of the penetration testing?	Yes
Wherever possible, please provide the breakdown of the count of servers, desktops, network, and security devices to be considered for vulnerability scanning, and then number of subnets?	As per the TOR

QUESTIONS & ANSWERS	
Questions from Service Providers	**Responses from NDA**
What is the expected frequency for conducting vulnerability assessment activities?	Bidder to recommend
Is there already a technology solution for vulnerability scanning and management? If yes, please describe the solution.	Yes
Do you require re-testing for the discovered vulnerabilities (High and Critical)?	No
Can the engagement be performed remotely by the penetration testers (where possible)?	Yes
no of screen= No of user roles= No of API with methods=	To be confirmed post contracting
Can we request one week's extension to the tender deadline?	No. The tender has been advertised for 22 days and this equates to one more days over and above the statutory requirement of 21 days.

Additional Comments

- The NDA is **NOT** looking for a service provider who sells cyber-security products or to implement cyber-security strategy.

SIGNED BY THE END USER AND SCM ON BEHALF OF BID SPECIFICATION COMMITTEE MEMBERS AS A TRUE REFLECTION OF THE CONTENT OF THE MEETING:

Mr Lunga Mbatha

SCM Unit

Mr Muzi Matsenjwa

SCM Unit

PP 

Ms Lerato Dhlamini

End User – ICT Unit