Independent Communications Authority of South Africa
350 Witch-Hazel Avenue, Eco Point Office Park
Eco Park, Centurion
Private Bag X10, Highveld Park 0169

APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY, INSTALL, CONFIGURE AND MAINTAIN A VULNERABILITY MANAGEMENT SYSTEM AND PROVIDE IT SECURITY HARDENING SERVICES FOR A PERIOD OF THREE (3) YEARS ON AN 80/20 PPPFA 2000, PREFERENTIAL PROCUREMENT REGULATION: 2017.

1. Background

With the rise in cyber security threats across the cyber space and more evolving threats constantly emerging, the organization's assets and data have become at risk. The need arises for a proactive approach in mitigating and preventing breach of data through continuous remediation of security vulnerabilities. Attackers constantly use new methods and techniques to evade detection and exploit vulnerabilities within the network to launch attacks such as man-in-the-middle attacks.

The vulnerability management system seeks to mitigate the risks by scanning the network for vulnerabilities and reporting and exposing the security flaws on the network before they are exposed to cyber-attacks.

2. Terms of Reference

Please refer to Annexure A for the Terms of Reference of the Vulnerability Management system and IT security hardening.

3. Period of Assignment

All work is to be carried out in accordance with the time schedule as agreed with ICASA. Supply, install, and configuring the system will be a once-off activity. Maintenance which shall include licensing of the software for a three (3) year period and remediation of the vulnerabilities on an ongoing basis for the duration of contract.

4. Briefing Session

There will be a compulsory virtual briefing session before the closing date. The briefing session will be done via Microsoft Teams. Prospective service providers will be required to mail the bid administrator requesting the link for the Teams session.

5. Bid Evaluation

The bid will be advertised for a period of 21 calendar days in the e-tender portal as well as the ICASA website.

Bidders will be evaluated on;
a) submission of the required documents,
b) functionality and
c) price/BB-BEE.

Only bidders who meet the cut-off score of 80 points out of 100 points for functionality will be considered further for price evaluation. All bid proposals submitted will be evaluated in accordance with the 80/20 procurement principle as prescribed by National Treasury Regulations.

Functionality Criteria per Category	**Weight**
Meets the functional requirements as per the scope of work on Annexure A.	**40**
Qualification and experience and proven track record in vulnerability management and remediation	**20**
Project plan submitted	**25**
Reference letters submitted	**15**
TOTAL	**100**

Annexure A – Terms of Reference

1. PURPOSE

The purpose of the bid is to appoint a service provider to supply, install, configure and maintain a vulnerability management system and provide IT security hardening service for a period of 3 years.

2. SUMMARY OF ENVIRONMENT

The ICT environment consists primarily of a data centre located at Head Office in Centurion with over 100 servers, Hyper-V and VMware virtualization, databases with mainly SQL, Oracle, PostgreSQL, Network devices consisting of Cisco switches, firewalls consisting of Cisco and Fortinet.
The environment can be summarised as follows

- It consists primarily of Windows and Linux servers,
- SQL, Oracle database as well PostgreSQL databases,
- Cisco firewalls, routers and switches,
- Centralized data centre,
- Eight (8) regional offices with their respective servers linked to the Head Office via an MPLS network.

3. PROJECT REQUIREMENTS

The bidder will be responsible for Installation, configuration, licensing, reporting, as well as maintenance of the Vulnerability Management system, including updates and patching of the system.

Bidders will be required to do continual remediation of security vulnerabilities and hardening for the 3 years of the contract. A key requirement will be that all vulnerabilities / risks that have been categorised as medium and higher must be attended to by the service provider during the first 90 days of the project. For the remainder of the contract duration, the lower rated vulnerabilities and any new vulnerabilities must be addressed. These remediations must be done after consultation with the ICASA IT team and after following the relevant ICASA change control approval process. In the compulsory briefing session, list of current vulnerabilities will be shared.

4. Mandatory requirements

#	Requirement				
1	Provide evidence to demonstrate that your organisation or solution provider adheres to good IT governance practices and complies with information security and privacy best practices. Examples ISO27001, ISO38500, COBIT The evidence can be in form of a certificate or letter from the relevant body.				
COMPLY	YES			NO	
Bidder should submit the supporting documentation:					

IF THE MANDATORY REQUIREMENTS ARE NOT MET, THEN BIDDER WILL BE DISQUALIFIED

5. Functional Requirements

The service provider will be required to provide a solution that satisfies the following requirements:

Section A -Vulnerability Management System functional requirements

*All requirements should be addressed in the proposal

#	Requirements				
1	Ability to schedule regular scans of up to 300 nodes.				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					
2	Subscription-based licensing model renewed on an annual basis				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					
3	Automated reports showing vulnerabilities and related risk profiles sent to relevant personnel on a regular basis				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained					

4	Out-of-the-box, pre-configured templates for IT and mobile assets, including configuration audits				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					
5	Automatic updates of plugins				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					
6	Broad, deep visibility into vulnerabilities covering network devices, operating systems, databases and applications.				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					

7	Create reports based on customized views (e.g., specific vulnerability types, vulnerabilities by host/plugin, by team/ client) – in a variety of formats (HTML, CSV)				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					
8	Ability to integrate with several commercial threat intelligence feeds for broader coverage				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					
9	Provide a broad range of plugins and coverage of CVEs				
COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					
10	Ability to provide unique custom audits to assist in compliance standards within the organization				

COMPLY	YES			NO	
Bidder should include a product specification/Datasheet and refer the section where the requirement is explained:					

No	Category	Weight
A.	**Price**	**80**
B.	**BBBEE Status Level Contribution**	**20**
	TOTAL	**100**

Section B - Evaluation Criteria

1.	**Vulnerability Management System Functional requirements** 5= complies with 10 functional requirements as per section A 3 = complies with 7-9 functional requirements as per section A 1=complies with less than 7 requirements	**40**
2.	**Provide a Project Plan to demonstrate how the current vulnerabilities will be addressed within 90 days and also how new ones will be addressed on an ongoing basis, including the plan of how the vulnerability management**	**25**

	system will be commissioned and maintained. 5 = A project plan with Milestones, Work Breakdown Structure, Schedule, Budget allocations, Responsibility Matrix 4 = A project plan with Milestones, Work Breakdown Structure, Schedule, Budget allocations, 3 = A project plan with Milestones, Work breakdown structure, schedule 2 = A project plan with only a schedule. 1 = Irrelevant plan or No project plan submitted	
3.	**Provide reference letters with client company letterheads for a similar service provided in the last 3 years.** 5 = Provide more than three reference letters of similar service supplied on client letterheads. 4 = provide three reference letters of similar service supplied on client letterheads. 3 = Provide two reference letters of similar service supplied on client letterheads. 2 = Provide one reference letter of similar service supplied on client letterheads. 1 = No submission of reference letter of similar service supplied on client letterheads.	**15**
4.	**Qualification and relevant experience of personnel working on the project.** • 5= 4 or more CVS with a combined experience in Windows, Linux, Oracle, SQL,	**20**

	PostgreSQL, CISCO, at least one personnel with CISSP certification and at least one with project management experience all with a combined minimum experience of 5 years. • 4= 3 CVs with a combined experience in Windows, Linux, Oracle, SQL, PostgreSQL, CISCO, at least one personnel with CISSP certification and at least one with project management experience all with a combined minimum experience of 5 years. • 3=2 CVs with a combined experience in Windows, Linux, Oracle, SQL, PostgreSQL, CISCO, at least one personnel with CISSP certification and at least one with project management experience all with a combined minimum experience of 5 years. • 2 =1 CV with a combined experience in Windows, Linux, Oracle, SQL, PostgreSQL, CISCO, at least one personnel with CISSP certification and one with project management experience all with a combined minimum experience of 5 years. • NO CVs submitted or All CVs with irrelevant experience	

	TOTAL FOR FUNCTIONAL PRE-QUALIFICATION CRITERIA.	**100**