ANNEXURE A – Terms of Reference

1. PURPOSE

The purpose of the Request for the Bid is to appoint a service provider to provide a Security Information and Event Management (SIEM) solution to the Authority. The solution should include system training for ICASA resources, licensing, software, hardware, maintenance and support over a period of 5 (Five) years. The hardware infrastructure will be on premise owned by ICASA with the service provider responsible for maintenance and support as well as 24/7 SOC for event analysis and reporting.

2. SUMMARY OF ENVIRONMENT

The ICT environment consists primarily of Windows and Linux servers with SQL and Oracle databases, Cisco devices and other network security appliances totalling approximately 160 event sources.

The environment can be summarised as follows

- Consists primarily of Windows and Linux servers
- Multiple SQL and 1 Oracle production databases,
- Cisco firewalls, routers and switches and other network security appliances totalling approximately 160 data sources. Head Office with centralized data centre,
- 8 regional offices with 2 servers each. Regional Offices connect via 4Mbps MPLS network.
- Average daily event rate of 75 000 000 events per day.
- Single domain with 3 AD servers at the head office and a read only DC at each Regional office.

Further sizing, storage and event rate information will be made available at the briefing session.

3. 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 ISO 27001, ISO38500 The evidence can be in form of certificate or letter from the certifying body stating the compliance thereof. Partners can also submit the evidence from the software vendor showing that the vendor does comply with the above.				
COMPLY	YES			NO	
Comment:					
2	Provide on-going system usage training for ICASA IT resources.				
COMPLY	YES			NO	
Comment:					

3	Provide all software maintenance and required patches for the SIEM solution for the duration of the contract.				
COMPLY	YES			NO	
Comment:					
4	Provide support hours to be used over the 5-year period				
COMPLY	YES			NO	
Comment:					
5	Database Activity Monitoring. The solution must be able to provide monitoring of administrator's activities within several databases (SQL & ORACLE) and provide regular reports of all the changes or modification by the administrators on what was modified, when, and by who. The monitoring can be directly through the SIEM solution and any other third-party module integrated to the SIEM solution.				
COMPLY	YES			NO	

Comment:

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

4. Functional Requirements

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

Section A -SIEM functionality

*All requirements should be addressed in proposal

#	Requirements				
1	Focuses on combining event data from disparate sources to assist with the identification of any suspicious activity and policy violations for the Authority's ICT environment.				
COMPLY	YES			NO	
Comment:					
2	Performs real-time monitoring of event data generated by workstations, network devices, security appliances, servers, databases and applications.				

COMPLY	YES			NO	
Comment:					
3	Contains a correlation engine to identify and detect patterns across the ICT environment with basic predefined correlation rules available at set-up to start analysing and correlating activity out-of-the-box that reduces false-positives automatically, detects authentication failures and operational events in real-time without the need to specify particular device types.				
COMPLY	YES			NO	
Comment:					
4	Can perform behavior profiling to identify anomalies and deviations from normal behavior.				
COMPLY	YES			NO	
Comment:					
5	Is user aware, i.e. identify the actual user of the source or destination, preferably through an Active Directory (AD) connection.				

COMPLY	YES			NO	
Comment:					
6	Provides customizable and consolidated reporting capabilities, from detailed daily reports to monthly reports and be capable of exporting reports in various formats.				
COMPLY	YES			NO	
Comment:					
7	Can retrofit virtually any application with logging capability that may not already be available and also provide a native out of the box capability to collect application log data from custom/in-house developed web applications, without explicit custom parser development.				
COMPLY	YES			NO	
Comment:					

8	Guarantees delivery of events to the log management system and that no events will get lost if the log management system is unavailable, even if the license has been exceeded, the solution must not drop incoming events.				
COMPLY	YES			NO	
Comment:					
9	Provides inline options to reduce event data at the source by aggregating event data. Aggregation must be flexible in which normalized fields can be aggregated and provide the ability to aggregate in batches or time windows.				
COMPLY	YES			NO	
Comment:					
10	Includes a module that can be used to provide compliance auditing, alerting and reporting for governances such as National Institute of Standards and Technology (NIST) Special Publication 800-53 and ISO/IEC 27002.				

COMPLY	YES			NO	
Comment:					
11	Natively integrate with existing authentication directories to import context related to users and roles which will then correlate and attribute every event to an actual user, regardless of the event source and be able to alert or report on any activity for identities not automatically synchronized with authentication directories.				
COMPLY	YES			NO	
Comment:					
12	Define whitelist/blacklists that can be used as inclusion or exemption during the correlation process. The correlation engine should utilize dynamic lists to provide important information such as shared user monitoring, session tracking, attack history and privileged system access.				
COMPLY	YES			NO	
Comment:					

13	Is capable of discovering patterns of subverted activities that would otherwise go unnoticed, i.e. slow and low attacks.				
COMPLY	YES			NO	
Comment:					
14	Provide the ability to import context and keep an inventory of all data as it relates to assets like hostname, IP & MAC address, business purpose, owner, vulnerability data, exemptions, compliance, criticality and other business-related data. The asset inventory must be able to integrate with vulnerability scanners to keep asset information up to date.				
COMPLY	YES			NO	
Comment:					
15	Is able to map IT Assets to Business Functions, and report on the Business Risk in the form of heat maps, reports, and scores against Key Performance Index (KPI).				

COMPLY	YES			NO	
Comment:					
16	Is capable of correlating activity between enterprise users and source code repositories. Users that are not developers accessing repositories or developers that are extracting sensitive intellectual property from the systems must be detected and alerted upon in real-time.				
COMPLY	YES			NO	
Comment:					
17	Is capable of allowing the restoration of a year's worth of historical log files to perform complex pattern searches and reporting against terabytes of data in a short period of time. The entire process from restoring the data to reporting results must take less than two days.				
COMPLY	YES			NO	
Comment:					

18	Provides the ability to visually represent event data into a dynamically updated graph to assist staff in determining the expanse of attacks and pinpoint the original attacker during incident response and remediation.				
COMPLY	YES			NO	
Comment:					
19	Provides out-of-the-box real-time detection and response capabilities on communications with known malicious hosts such as botnet and/or other hosts on the Internet known to host/facilitate data exfiltration by malwares.				
COMPLY	YES			NO	
Comment:					
20	Is capable of triggering scripts or execute integration commands with third-party solutions, Next Generation Intrusion Prevention systems in order to quarantine or block malicious activity in real-time.				

COMPLY	YES			NO	
Comment:					

Section B – SIEM Reporting

1	Capable of producing reports that monitor activities of IT administrators and report on their activities within servers hosting services such as Active directory, SQL databases, Oracle databases, Windows logon events, Linux OS logon events.				
COMPLY	YES			NO	
Comment:					

2	Be able to produce daily reports of all activities within the network for a 24-hour period covering aspects such as: Malware & Anti-virus activities. Suspicious traffic to malicious sites, backdoor or Torrent ports Perimeter Security scans and exploits. AD security correlated events- Failed and Lockout accounts including service accounts, multiple host logging from single AD account, Brute force attempts from a single source. Correlated internal reconnaissance events, horizontal scans.

COMPLY	YES			NO	

Comment:

3	Be able to produce weekly reports of all activities within core servers: Weekly Active Directory activities report. Weekly Linux server login report. Weekly Windows server logon activities. Weekly SQL and Oracle databases activity reports.				
COMPLY	YES			NO	
Comment:					
4	Be able to produce alerts for the following incidents: Active Directory group policy violation change. Firewall rules changes. Suspicious traffic to malicious sites. Alerts from the McAfee ePO on antivirus events.				
COMPLY	YES			NO	
Comment:					

5	Be able to produce Monthly security overview report showing aspect such as: Monthly Risk rating and three-month trend security posture. Malware overview report based on McAfee endpoint protection. Top account login failures. Top account lockouts. TOR/Back-door traffic overview Perimeter security overview Overview of incident reported during the month and SLA monthly report				
COMPLY	YES			NO	
Comment:					

5.Bid Evaluation

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.

Functionality Criteria per Category	**Weight**
Meets the requirements as per the scope of work, Annexure A.	**80**
Experience and proven track record with SIEM technology	**20**
TOTAL	**100**

Meets the FUNCTIONAL requirements as per the scope of work, Annexure A, Section A

No	Section A - SIEM Functionality	Score
1	Meets 18-20 of the requirements as stated in Annexure A, section A	5
2	Meets 16-17 of the requirements as stated in Annexure A, section A	4
3	Meets 13-15 of the requirements as stated in Annexure A, section A	3
4	Meets 10-12 of the requirements as stated in Annexure A, section A	2
5	Meets less than 10 of the requirements as stated in Annexure A, section A	1

60

Meets the FUNCTIONAL requirements as per the scope of work, Annexure A, Section B

No	Section B – SIEM Reporting	Score
1	Meets all 5 of the criteria as stated in Annexure A, section B	5
2	Meets 4 of the criteria as stated in Annexure A, section B	4
3	Meets all 3 of the criteria as stated in Annexure A, section B	3
4	Meets all 2 of the criteria as stated in Annexure A, section B	2
5	Meets all 1 of the criteria as stated in Annexure A, section B	1

20

Experience and proven track record with SIEM technology

No	Reference Letters	Score
1	4 or more reference letters from the client detailing similar service rendered in the last five years	5
2	3 reference letters from the client detailing similar service rendered in the last five years	4
3	2 reference letters from the client detailing similar service rendered in the last five years	3
4	1 reference letter from the client detailing similar service rendered in the last five years	2
5	No reference submitted	1

20