ANNEXURE 3

SUPPLY CHAIN MANAGEMENT

1. **INTRODUCTION**

The purpose of this bid is to appoint a service provider who can establish an enterprise-wide security information and event management solution ("SIEM") in the form of a Security Operations Centre ("SOC") as a managed service.

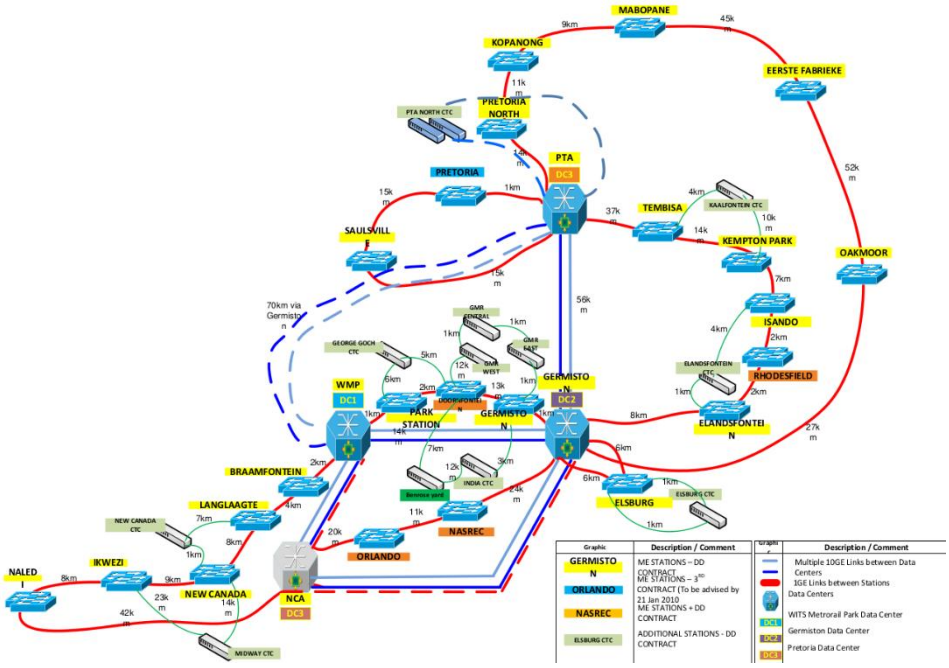
The Service Provider needs to:

- Implement a logging, monitoring and alerting solution (SIEM).
- Run and manage the solution and capabilities for 36 months.
- Offer a continuous service in the form of managed security service SOC.

2. BACKGROUND INFORMATION

As part of PRASA's ICT Security Strategy tabled in 2021, the objective is to establish a capability within PRASA to collect and monitor security related system activities, to allow PRASA to monitor for cyber security intrusions and incidents, within its critical IT and OT infrastructure environments.

PRASA's technology landscape is distributed across multiple data centres, offices and stations. Primary data centres are in Gauteng, KwaZulu-Natal and the Western Cape.



The most notable data services can be broken down into three different classes:

Business Services

These are the services, which allow local and remote user's access to applications, as well as the transport of Datacentre (DC) application data external to the DC for application communication, data backup, Business Intelligence etc.

ICT Services

These are the services that PRASA internal users require to complete their day-to-day responsibilities. Examples are SAP, email, internal LAN access, file and print functions, Intranet as well as Internet access, and multimedia communication (telephony, video conferencing, document collaboration etc.).

Operational Services

These are the customer facing services which PRASA is deploying to support the business operation and improve the commuter experience. Examples are:

Ticketing, CCTV, PA systems, Digital signage, Public Help Points, Access Control, Wireless communications to the new trains etc.

From an IT systems point of view, the following appliances, applications, operating systems and management software can be found within PRASA.

SERVICE COMPONENTS	TECHNOLOGY USED
LAN/MAN	Cisco switches (catalyst 3560, 6500, 7600), MPLS, Metro-Ethernet
Firewall	Cisco ASA 5540
Proxy	Sophos XG450
Server Hardware	CISCO UCS VBlock200, HP DL380–980 Generations (Wintel), And Oracle Super Cluster T5-8 and Sun MSeries servers (ERP)
Operating Systems	Server: Windows 2003/2008/2012/2019, Linux and Solaris
Directory	MS Active Directory 2016 (countrywide)
WAN	MPLS through Internet Solutions
File/Print	Windows 2003/2008/2012/2016
Document Management	Hummingbird/Open Text/SharePoint
Backup	Veritas Netbackup, HP StoreOnce 4500 and Netbackup Appliance 5230
Storage	EMC VNX and Clarion CX3, HP 3PAR, other
Email System	Exchange online
Terminal services	Citrix
Remote Access	MTN APN, Vodacom, Cisco VPN client and IPsec
Virtualization	VMware, Oracle VM
Database	MS SQL, Oracle
ERP	SAP, Empac, FMMS, HR, PP, FIN

Anti-virus	Kaspersky, Windows Defender
Telephony	Cisco IPT, Unity, Rightfax
Datacentre	6 Datacentres (Pretoria, Johannesburg, KZN, WC, EC, GNC)
Data Center Management	APC ISX technology
Environmental Monitoring	Netbotz
CCTV	Dallmeier,
Access Control	Babylon
Structured Cabling	ADC Krone CAT6 (TE Connectivity)
Fibre Infrastructure	ADC Krone (TE Connectivity) Splice Trays : Single-Mode – Use LC-APC Connectors Multi-Mode – Use LC –PC Connectors
Other	Office 2007/2010, CA Helpdesk System, Microsoft SCOM and SCCM, Various Rail Specific Applications Office 365 with E3 license

The number of endpoints can be summarised as follows:

- Laptops = +-850 (Windows 7 – Windows 10)
- Desktop =+-2000
- Windows Servers = 218 (versions 2008 - 2016)
- Linux/Solaris = +-100
- Web servers = +-10

3. OBJECTIVE OF THE PROPOSED PROJECT

The objective of the RFP is to solicit bids from suitably qualified service providers with the purpose of implementing a security information and event management (SIEM) capability, together with a managed services component in the form of a SOC.

The service provider is to provide log collection, monitoring, analysis and alerting across a variety of technologies and platforms within PRASA. The service provider will have to deploy collection devices (hardware or software) and reconfigure existing reporting devices to supply logs to the collection devices (on-host agents or system native forwarding capabilities e.g., rsyslog). The placement of the log collection platform should not in any way adversely affect the bandwidth of PRASA.

The service provider would be required to ensure the capability becomes a standard operating procedure within PRASA.

4. SCOPE OF WORK AND AREAS OF FOCUS

4.1 The successful Bidder would be required to implement the following capabilities for PRASA in a managed services format:

- Log collection and correlation.
- Continuous monitoring and alerting.
- Continuous vulnerability scanning.
- Use case and playbook development and maintenance.
- Threat intelligence collection and data enrichment.
- Incident response and incident containment.
- Forensic investigations.

4.2 The successful Bidder will recommend an approach to enable the above-mentioned capabilities, by consuming security event logs from workstations, servers, databases and network perimeter devices in such a way to illustrate proof of value in the shortest space of time. Initial log sources must include a selection of authentication services (Active Directory), firewalls and proxies, DNS, staff workstations and application server

logs. The initial number of devices should not exceed 100 devices, to ensure shorter delivery time.

4.3 Even though the initial implementation for proof of value will be limited, the solution and service must be able to eventually deal with a 200GB of raw data logs per day.

4.4 The event monitoring and alerting service will be offered as a 24 hours per day, 7 days a week service.

4.5 The SIEM must be implemented on-premises (within the PRASA data centres).

5. SPECIFICATION OF THE WORK OR PRODUCTS OR SERVICES REQUIRED

ANNEXURE 3 A details the general solution and service compliance requirements.

Meeting all requirements in Annexure 3 A are mandatory and Bidders must sign the necessary sections to indicate and confirm their contractual obligation to provide these services and features at the time the bid is awarded.

Failure to meet all requirements or signing the required sections where indicated will result in the submission being disqualified.

6. CONTRACT DURATION

36 months

Bidders must provide a breakdown of the costing to PRASA based on the Pricing Schedule in **ANNEXURE 3 B**.

7. *EVALUATION PROCESS*

Interested bidders for this project shall be evaluated in terms for their administrative responsiveness, substantive responsiveness, technical/functional (capacity testing) evaluation and preference points..

EVALUATION PROCESS	
Stage 1A - Compliance	Mandatory Compliance Requirements (Substantive Responsiveness)
Stage 1B - Compliance	Basic Compliance Requirements (Administrative Responsiveness)
Stage 1C – Compliance	General solution and service compliance
Stage 2	
Technical/Functional Criteria	Testing of capacity – meet minimum threshold of 70%.
Stage 3 **Preference Points**	
Price	80
BBBEE	20
TOTAL	***100***

STAGE 1 - Mandatory and Basic Compliance Requirements (Substantive and Administrative Responsiveness)

No.	**Description of requirement**	
Stage 1A - Mandatory Compliance Requirements (Substantive Responsiveness) If a supplier / bidder does not submit the following documents the Proposal will be disqualified automatically:		
a)	Completion of ALL RFP documentation (includes ALL declarations, ALL Standard Bidding Documents (SBD) and Commissioner of Oath signatures required)	

No.	Description of requirement	
b)	Signed Joint Venture, Consortium Agreement or Partnering Agreement, if applicable.	
c)	Company registration documents	
Stage 1B - Basic Compliance Requirements (Administrative Responsiveness) If you do not submit the following basic compliance documents your bid may be disqualified and these documents must be made available within a specified period should an award, be made: e.g 7 days		
a)	Original or certified B-BBEE certificate issued by SANAS (Certificates issued by IRBA and Accounting Officers have been discontinued, however valid certificates already issued before 1 January 2017 may be used until they phase out completely by December 2017) Bidder to include Affidavit for QSEs and EMEs. In cases of JVs or consortiums, a combined B-BBEE certificate in the name of the JV/Consortium must be submitted	
b)	CSD supplier registration number *(should a bidder not registered on CSD, the bidder will be afforded 14 days after the closing date to register accordingly)*	
c)	A valid and Original Tax Clearance Certificate (valid as at the closing date of this RFP) Or supply SARS Pin	
d)	Latest financial statement	
e)	Copies of Directors' ID documents	
f)	Letter of Good Standing: COID	

Stage 1C – Technical Mandatory Compliance

Technical Mandatory Compliance Annexure A.

Meeting all requirements in Annexure A are mandatory and Bidders must sign the necessary sections to indicate and confirm their contractual obligation to provide these services and features at the time the bid is awarded.

Failure to meet all requirements or signing the required sections where indicated will result in the submission being disqualified.

STAGE 2 - TECHNICAL / FUNCTIONALITY REQUIREMENTS

Qualifying bidders shall be evaluated on technicality / functionality after meeting all compliance requirements outlined above. The minimum threshold for the technical/functionality requirements is 70%. Bidders who score below the minimum requirement shall not be considered for further evaluation in **Stage 3.**

Details of the scoring methodology presented above are outlined below:

ITEM	CRITERIA	WEIGHT	SCORES
1	**Project Management Skills and Experience Consider the option of certification**	20	The bidder is required to provide the detailed Curriculum Vitae of the Project Manager who will be assigned to the project who has acquired the following certification and skills: a. Experience in onboarding managed security services and SOC projects with a minimum of 1000 managed devices. Note: i. *PMP, PMBPOK or Prince2 Certificates must be provided with the Project Managers' CV to be awarded points for this evaluation criteria.* *ii. Relevant post certification experience which can be verified.* No response received = 0 points awarded 1 and more years and less than 2 years' Post Certification Experience in the management of projects of scope and size as highlighted in Point "a" above and supporting of services in the scope of the project = 1 point awarded. 2 and more years and less than 4 years Post Certification Experience in the management of projects of scope and size as highlighted in Point "a" above and supporting of services in the scope of the project = 2 points awarded.

ITEM	CRITERIA	WEIGHT	SCORES
			4and more years and less than 6 years Post Certification Experience in the management of projects of scope and size as highlighted in Point “a” above and supporting of services in the scope of the project = 3 points awarded. 6 and more years and less than 7 years Post Certification Experience in the management of projects of scope and size as highlighted in Point “a” above and supporting of services in the scope of the project = 4 points awarded. 7 and more years Post Certification Experience in the management of projects of scope and size as highlighted in Point “a” above and supporting of services in the scope of the project = 5 points awarded.
2	**Active years providing managed security services in the form of a SOC**	30	The Bidder must at least have been in operation for a period of 3 years from the closing date of this bid. Bidders must provide confirmation in the form of a signed letter on the company letterhead as proof. No response received = 0 points awarded. Managed SOC services in operation for less than 2 years = 1 point awarded. Managed SOC services in operation for more than 2 years and less than 3 years = 2 points awarded. Managed SOC services in operation for 3 and more years and less than 5 years = 3 points awarded. Managed SOC services in operation for 5 and more years and less than 7 years = 4 points awarded. Managed SOC services in operation for more than 7 years = 5 points awarded.
3	**Contactable case references**	30	The Bidder must submit reference letters or completion certificates from previous /present clients where SOC solutions and services were rendered. PRASA reserves the right to contact these references. All letters must be on a company letterhead and signed by the client. The client must be contactable, and the contact details provided.

ITEM	CRITERIA	WEIGHT	SCORES
			No response received = 0 points awarded. 1 contactable reference received = 1 point awarded. 2 contactable reference received = 2 points awarded. 3 contactable references received = 3 points awarded. 4 contactable references received = 4 points awarded. 5 or more contactable references received = 5 points awarded.
4	**Project Delivery Leadership and Qualifications to deliver the service.**	20	All Bidders must have the relevant knowledge, human resources, and capacity to deliver the services required. Bidders must provide CVs that contain project team member qualifications, certifications, and years' experience in the field of security monitoring and incident management. The CVs should reference the following team member capabilities and experience: a. SOC manager with at least three (3) years' experience in the Security ICT environment managing a SOC. b. SOC analysts with at least three (3) years' experience in the Security ICT environment and SOC environment. c. Security engineers with capability (product certification or training) to implement and maintain the SIEM software to be used by the SOC analysts. No CVs received = 0 points awarded. CVs received indicating a SOC manager with less than 2 years' experience in managing a SOC; 1 SOC analysts with 1 years' experience; 1 security engineer with suitable solution support capability = 1 points awarded. CVs received indicating a SOC manager with 2 and more years' experience in managing a SOC; 2 SOC analysts with 2 years' experience; 1 security engineer with suitable solution support capability = 2 points awarded. CVs received indicating a SOC manager with 3 and more years' experience in managing a SOC; 2 SOC analysts

ITEM	CRITERIA	WEIGHT	SCORES
			with up to 3 years' experience; 1 security engineer with suitable solution support capability = 3 points awarded. CVs received indicating a SOC manager with more than 3 years but less than 5 years' experience in managing a SOC; 3 SOC analysts with 3 and more years' experience; 2 security engineers with suitable solution support capability = 4 points awarded. CVs received indicating a SOC manager with more than 5 years' experience in managing a SOC; 3 SOC analysts with more than 3 years' experience; 2 security engineers with suitable solution support capability = 5 points awarded.

STAGE 3 - Pricing and BBBEE

Pricing Evaluation: Only Bidders who have achieved the 70% threshold for technical evaluation will be evaluated for BBBEE and Price.

BEE Evaluation: The B-BBEE component of evaluation is weighted at 20% of the evaluation criteria. Determination of points of B-BBEE is based on the B-BBEE Recognition Level as per table below:

CATEGORY	80/20 PREFERENTIAL POINT SYSTEM	CATEGORY	Points
Price	80	1	20
		2	18
		3	14
BBBEE Level Contributor	20	4	12
		5	8
		6	6
		7	4

		8	2
		Non-Compliant Contributor	0

The formula for calculating price scores is as follows:

$$Ps = 80\left[1 - \frac{Pt - Pmin}{Pmin}\right]$$

Where

Ps = Points scored for price of tender under consideration

Pt = Rand value of tender under consideration

Pmin = Rand value of lowest acceptable tender

Failure to submit valid and original (or a certified copy of) proof of the Respondent's compliance with the B-BBEE requirements stipulated in this RFP (the B-BBEE Preference Points Claim Form) at the Closing Date of this RFP will result in a score of zero being allocated for B-BBEE.