Electoral Commission

Auction # XXXXXXXX

LGE 2021 –Security Operations Centre

IMPORTANT NOTICE

Failure to comply with the completion of the auction conditions and the required information or submission of the required stipulated documents indicated above (i.e. non submission of the required documentation) shall invalidate a bid.

1. Purpose

The Electoral Commission (IEC) seeks to procure the services of a service provider to run an additional parallel Security Operations Centre (SOC) for a period not more than 3 months during the Local Government Elections (LGE) 2021. This will form part of the integrated security monitoring and response teams and infrastructure. The services will include providing real-time security information and events monitoring systems and personnel over a specified period.

Bidders must place a bid on the Votaquotes (e-Procurement) system and then provide all the required documentation before the due dates as specified in this document and on the Votaquotes web site.

2. Background Information

The Electoral Commission has invested extensively in ICT technologies, which provide a platform to effectively support and enable its business processes, in an effort to meet its goal of delivering free and fair elections in an open and transparent environment. The Electoral Commission's ICT Department intends to continue running a highly efficient, stable and secure ICT infrastructure, making full use of industry standards, best practices and disciplines based upon stable and reliable technologies.

The Electoral Commission has adopted a net-centric architecture that operates on a wide area network connecting more than 300 offices at various locations around the country and around 2000 users, using a combination of platforms including a private network. In addition, the IEC has an extensive online presence with various websites and web portals including mobile applications, which provides real-time and online data processing capabilities in various forms.

3. Technical Specifications

The technical specification for the required solution is as specified below. It must be noted that the technical specifications below are the minimum requirements; the only deviation that may be accepted will be in case where the bidder's specification is better. Anything below specification will be disqualified. The bidder is required to provide a detailed methodology for the testing of all of the following security assessment requirements.

3.1. Overview of the Electoral Commission's ICT Environment

The Electoral Commission's National Office is located in Centurion and in various remote sites countrywide:

a) National office: The IEC has adopted a centralized architecture, with a data-center at national office, all major computing equipment are deployed and processing from the data-center.

b) The national data-center has over 100 physical and virtual servers, including associated data-center computing equipment such as storage systems, backup systems, networking, security, etc.;

c) Disaster recovery (DR) site: An alternative site hosting a business continuity and disaster recovery capability for key critical systems, the disaster recovery site also caries similar computing capability as the national data center, although at a lower scale and capacity.

d) Provincial offices: nine (9) offices country wide hosting a number of servers and an average of thirty (30) workstations, located in each of the 9 South African provinces;

e) Warehouses, ten (10) warehouses country-wide, one in each province and one at national level, hosting between two (2) and thirty (30) workstations;

f) Local municipal offices: approximately three hundred (300) offices countrywide hosting an average of three (3) computers with routers and switches.

g) Network structure: The Electoral Commission uses Virtual Private Network service to provide connectivity to the entire wide area network (WAN) with Voice-Over-IP capability at some sites.

h) During election period, that is during the period envisaged for this service, the network gets expanded to connect an additional data-center at the national results operations center, additional sites such as 9 provincial results operations centers and various results capturing sites at the municipal level averaging around 50.

i) During the elections, the Electoral Commission's website gets hosted at an Internet Service Provider (ISP).

3.2. Overall Technical Capability Requirements

The bidder must have skill, experience and technological systems and tools to be able to deliver on the following capabilities:

a) **OWASP Top 10** web and mobile security risks – deal with 10 of the most common threats to web and mobile applications as identified by Open Web Application Security Project (OWASP)

b) **Ingest** – All data to determine security relevance. The ability to ingest data from any source, structured or unstructured, at scale and the ability to organize that data to make it actionable by machine or human.

c) **Detect** – The ability to detect security event.

d) **Predict** – The ability to predict a security event allows the SOC to proactively escalate the incident to a human or to streamline a response with a predefined process.

e) **Automate** – Usage of automation tools to take standard operating procedures and turns them into digital playbooks to accelerate investigation, enrichment, hunting, containment and remediation.

f) **Orchestrate** – The ability to plug in and connect everything that is inside and outside of your SOC.

g) **Recommend** – The ability of the platform powering the SOC to tell the analysts what to do next by making a recommendation.

h) **Investigate** – Investigation requires detailed, precise analysis with the assistance of intuitive security tools which can prioritize what needs to be investigated.

i) **Collaborate** – Security requires coordination, communication and collaboration including the ability to collaborate and connect the tools, people, process and automation into a transparent workplace, bringing information, ideas and data to the forefront and enabling security teams to better collaborate.

j) **Manage** – The ability to arm security teams with everything necessary to manage the response process when incidents have happened.

k) **Report** – Having the right reporting tools helps inform on what's performing, so

security teams can accurately measure where they are and where they need to go.

The bid must demonstrate the bidder's skills, experience and capacity to deliver along these capabilities in providing security operations centre services.

3.3. Information Security Monitoring Requirements

Technical requirements for the security operations center must include the following:

a) The service provider is to monitor the Electoral Commission's hosting facility, National Office, DR Site and the National and Provincial Results Operations Centers (ROCs) and the entire wide area network (WAN) from one central site (National Office).

b) Log management; user and entity behavior analytics (UEBA); and security orchestration, automation, and response in a complete, end-to-end security operations platform.

c) The ability to collect massive volumes of data in real time, using such technologies such as machine learning algorithms to detect advanced threats, and provide artificial intelligence-based security incident response capabilities for fast remediation

d) Sources of security information and events must include firewalls, intrusion prevention systems, antivirus and antimalware software, data loss prevention tools and secure web content gateways.

e) The service provider must have credible and advanced security monitoring systems and tools. The service provider must include data sheets or more information about the products proposed for the project.

f) The bidder must provide their own log management or SIEM solution. The bidder may be allowed to access the Electoral Commission's existing Security Incident and Events Management (SIEM) system.

g) The data collected over the contract period belongs to the Electoral Commission and must be made available to the Electoral Commission at the end of the project before being purged by the service provider. The service provider must

confirm that the data has been purged and the disk drives are defragmented to disable data recovery.

h) The service provider will be required to utilise their own security monitoring solutions. The use of Security Orchestration, Automation and Response (SOAR) tools will be an added advantage.

i) The bidder must indicate which tools they will be using; the tools will have to monitor for any Cyber and networking security related events including but not limited to the following:

1) All security and network related events and attacks
2) Account and password guessing attacks
3) User access monitoring
4) User and Entity Behavior Analysis
5) Account modification (e.g. account lockouts, password by non-owner)
6) Privilege account creation and modification (and escalation)
7) Switch configuration changes
8) Firewall configuration changes
9) Malware / Bot monitoring
10) IPS event monitoring
11) Port & vulnerability scan detection
12) DDOS monitoring / alerting
13) Malware infections and propagation
14) Unauthorized network access attempts (via Ethernet, Wi-Fi and any other mechanism)
15) Authorized penetration test and vulnerability scanning websites and applications
16) Network performance monitoring utilizing the Electoral Commission's monitoring tools
17) Remediation on request

j) All security logs and vulnerability information must remain on-premise;

k) Monitoring of security events and logs of critical devices and overall network security posture (numbers may vary depending on requirements);

l) Collected events data should support forensic investigations when required;

m) Security events and logs must be aggregated and collated to a central monitoring solution and computer emergency response must be aligned with the incident criticality. The Electoral Commission's designated resources need at least view access to the central monitoring solution or dashboard;

n) The total project duration will not exceed three (3) months inclusive of set-up, fine tuning, operations, monitoring and decommissioning;

o) 24x7 Monitoring and incident response required for a period of one (1) month – election month;

p) Two (2) resources required onsite 24x7 for a period of two weeks, from a week before Election Day to after the announcement of results. Ordinarily results announcement is done on the fourth day after election day;

q) Provide an incident response plan indicating the incident logging procedure, allocations and classification of logged incidents and the escalation procedure;

r) Reporting on a daily and weekly basis as well as a full report at the end of the project. Timeous reporting during the critical days.

s) A health check and rule review will be required as well as fine tuning of current rules and new rules sets. The bidder takes full accountability and responsibility for the accuracy of incident monitoring, reporting, alerting and commissioning of existing and new devices.

t) Bidder must provide a close-out report at the end of the project

3.4. Special Requirements

a) Latest cyber security monitoring, vulnerability integration, log management, security orchestration, automation and response methodologies, techniques and tools are required.

b) A plan detailing the tools to be used and the processes and procedures to be followed must be submitted as part of the bid response.

c) The winning bidder will be required to enter into a Non-Discloser Agreement (NDA) with the Electoral Commission.

d) The bidder must be certified and accredited in the tools and solutions they are proposing to use.

e) The bidder's personnel to be deployed on the project must have the necessary professional qualifications and certification in this area of security including but not limited to CompTIA Security+ and CompTIA Cybersecurity Analyst

f) The Electoral Commission reserves the right to reduce the scope of the project depending on such factors as the time and/or budget available, risk exposure and other factors

3.5. Delivery and Implementation Timeframe

a) The successful bidder will need to have a flexible and adjustable process as the delivery will be during election.

4. General Auction Conditions

The following standard auction conditions must be adhered to and complied with, failing of which the bid will be disqualified.

a) To demonstrate capacity and experience the bidder must submit at least two (2)curriculum vitae (CV) for their staff with the necessary professional qualifications and certification in this area of security including but not limited to CompTIA Security+ and CompTIA Cybersecurity Analyst and having preferably 3 years or more cybersecurity and networking experience;

b) The bidder must clearly state the details of services in their technical proposal (including architecture, tools, reports, monitoring and compliance approach, use of artificial intelligence, machine learning etc.) to be supplied;

c) All costs of delivering this service will be for the bidder, no additional costs outside the bid price will be considered;

d) The bidder must state the following:

(i) licensed tools to be used

(ii) list the qualifications of project team members

(iii) Partnerships and Associations

e) The successful bidder and their project team members may be subjected to security clearance assessment by the relevant state security institution. It must be noted that non-South African citizens are unlikely to receive security clearance and are therefore not recommended.

f) The bidder must be able to demonstrate experience doing similar engagements with similar clients by providing three (3) references, contact details, description of the services, period of the project, number of staff worked on the project.

g) The bidder should demonstrate an understanding of the relationship between business needs and information security requirements;

h) The bidder must supply an implementation project plan stating scope, milestones, risks, deadlines (durations), roles and dependencies for the successful delivery of the required services;

i) The bidder must suggest a project governance structure including Steering Committees and Project Committees and the frequencies of meetings

j) The Electoral Commission will issue a formal purchase order to the successful bidder before any services can be delivered;

k) Awarding of the auction to any successful bidder may be subject to the Electoral Commission's due diligence audit requirements, where applicable;

l) No payment shall be made until all deliverables have been delivered in accordance with the bid specifications.

m) The service will be delivered during elections at a date to be confirmed

n) While the proposal must be able to stand on its own, the bidder must state all their requirements and/or dependencies on the Electoral Commission and its infrastructure.

5. Quality Control

The following quality control conditions must be adhered to and complied with, failing of which the bid will be disqualified.

a) The bidder must undertake and warrant that services are in line with auction specifications.

b) The successful bidder will have the primary responsibility of ensuring that the proposed services comply with the required specification in terms of functionality and technical specification including quantity and quality
c) It must be noted that the Electoral Commission seeks to gain the best solution technically, functionally and financially, and will select the solution that it deems to give the best investment
d) Preference will be given to services that are based on existing solutions in the market and not products specifically designed and/or cloned for this bid.
e) The successful bidder has the primary responsibility to ensure that the quality of their submission is in accordance with the bid specifications.

In addition, the Electoral Commission may also call on bidders to make further submissions and/or presentations in order for the Electoral Commission to ensure full compliance with all its requirements and as part of the auction evaluation process prior to the conclusion of the adjudication of the auction.

6. Pricing requirements

When pricing bid proposals, bidders are advised to take into account that all items required to establish and maintain a SOC are factored into the price. A detailed breakdown must be provided to make it possible to adjust services and costs should the need arise. Where possible the breakdown must include personnel hourly rates, usage of tools and equipment where-ever possible or required.

The bid price must be all inclusive for the proposed services, there should be no dependency on additional costs, additional optional items applicable can be listed and submitted but should not be such that the service cannot be delivered without the optional items.

The price breakdown must include the following:

a) Setup, installation and configuration including running for a period in learning mode and fine tuning;
b) Security monitoring services;
c) Device rental or usage costs
d) Personnel costs including their hourly rates
e) Any software licensing costs, if any

f) Travel costs if applicable, etc.

7. Award of Order

a) The order will be awarded to a bidder whose solution successfully conforms to specifications and is able to deliver and support the product, and in terms of the provisions of the Preferential Procurement Policy Framework Act, 2000
b) The successful bidder may also be required to enter into a Service Level Agreement (SLA/Contract) with the Electoral Commission in order to formalize and confirm the exact solutions to be delivered
c) The Electoral Commission will issue a formal order before any services can be delivered
d) It should be noted that the Electoral Commission seeks to gain the best solution technically and financially and will select from the results of the auction a solution it deems to give the best investment

8. Written Submissions

A written proposal on the proposed services with all supporting documentation is required. The written submission must be clear on what the bidder is offering through their bids and must address and explain at least the minimum requirements in the specifications. The submission must be brief, comprehensive and adequate to enable the Electoral Commission to objectively assess the bid and verify compliance with auction conditions and specifications.

All submissions must be received on or before the closing date and time as stipulated in this auction. Submissions received after the final date and time shall lead to bids being disqualified and not considered.

Written submissions must be delivered to the Electoral Commission's Procurement & Asset Management Department. Delivery can be through any of the following means before the closing date and time:

- Uploading on the auction

- Place in the Commission's tender box situated in the foyer of the Electoral Commission's national office in Pretoria at the following address:

  Election House
  Riverside Office Park,
  1303 Heuwel Avenue,
  Centurion,
  0157

Note: Clearly mark your submission: For the attention of Procurement and Asset Management – Auction XXXXXXXX

In addition, the Electoral Commission may also call on bidders to make further submissions and/or presentations in order for the Electoral Commission to ensure full compliance with all its requirements and as part of the auction evaluation process and prior to the conclusion of the adjudication of the auction.

Failure to submit all of the required documentation (see summary list of submission points below) before the closing date and time will invalidate the bid. It remains the responsibility of the bidder to confirm receipt of the required documentation with the Electoral Commission Procurement department.

Summary list of submission requirements:

a) Written proposal of the service offering, methodology, architecture, tools, reports, monitoring and compliance approach, use of artificial intelligence, machine learning etc,and adherence to the auction technical specifications as stipulated in sections 3.2 and 3.3.

b) Track record - List of three (3) contactable reference customers, as per section 4 (f)

c) Staff experience and knowledge. Two (2) CVs of staff with relevant experience and relevant qualifications as per section 4 (a) and 4 (d).

d) Project Plan, as per section 4 (h).

e) Incident Response Plan, as per section 3.3 (q)

f) Governance Structure as per section 4(i)

g) Proposal must specify systems and tools to be used including dependencies as per clause 4 (d)

9. Closing Date

The closing date and time of this auction is specified on the e-Procurement (Votaquotes) website. The closing date and time is determined by the clock on the Electoral Commission's servers and is not negotiable. Bidders must also take note that supporting documentation must be delivered as specified on the auction.

Auction XXXXXXXX
Security Operations Centre (SOC)

Bidder:	
Date of Bid Evaluation:	

Phase1 – Accreditation of Bidder **Qualifying / Disqualifying Factors** **Failure to comply with below requirements shall lead to bid disqualification.**			
No.	**Description**	**Yes/No***	**Comments**
1	Written proposal detailing service offering, methodology, architecture, tools, reports, Monitoring and compliance approach, use of artificial intelligence, Machine learning etc. of the solution provided also indicating compliance to the auction technical specifications as per sections 3.2 and 3.3		
2	Track Record - Three (3) Contactable References, as per section 4 (f)		
3	Staff experience and knowledge. 2 x staff CVs with relevant experience and relevant qualifications, as per section 4 (a) and 4 (d)		
4	Project Plan, as per section 4 (h)		
5	Incident Response Plan, as per section 3.3 (q)		
6	Specified tools, as per section 4 (d)		

Result of phase 1: Bid qualifies/does not qualify for further consideration.

.

Phase 2 – Technical Evaluation Criteria Bidders must score a minimum of 75% (62/83) to proceed to the next evaluation phase					
	Description		**Weighted Score**	**Score**	**Comments**
1	Written proposal detailing service offering, methodology, architecture, tools, reports, monitoring and compliance approach, use of artificial intelligence, machine learning etc. of the solution provided indicating adherence to the auction technical specifications	(a) Architecture, system components including list of tools to be used = 17 points i. Detailed description of the solution architecture, (**2 points)** ii. Detailed description of the solution capabilities in regards to: (**10 points**) I. Ingest (1 point) II. Detect (1 point) III. Predict (1 point) IV. Automation, (1 point) V. Orchestrate (1 point) VI. Recommend, recover and remediate (1 point) VII. Investigate (1 point) VIII. Collaborate (1 point) IX. Manage cases (1 point) X. Report (1 point) iii. Detailed description of all the system components including tools (SIEM, SOAR, Dashboard, Integration Mechanisms with existing infrastructure etc.) (**5 points**) I. 4 or more tools = 5 points II. 2 or 3 tools = 3 points III. 1 tool = 1 point IV. No tools = 0 point (b) Methodology, Monitoring and Compliance Approach, details of how the services will be provided (**6 points**) i. Threat Detection Approach (3 points) ii. Incident Response Approach (3 points)	38		

Phase 2 – Technical Evaluation Criteria Bidders must score a minimum of 75% (62/83) to proceed to the next evaluation phase					
	Description		**Weighted Score**	**Score**	**Comments**
		(c) The use of User and Entity Behavior Analytics (UEBA) and Artificial Intelligence tools to intelligently detect and respond to anomalies = **10 points** i. Description of UEBA Approach =2 point ii. Network Activity Monitoring approach=2 points iii. Login Attempts Monitoring =2 points iv. Removable media =2 points v. Description of evaluation and scoring of threats mechanism =2 points (d) Provision of data sheets / more information on the tools used for the project = **5 points** i. 4 or more data sheets =5 points ii. 3 data sheets =3 points iii. 2 data sheets =2 points iv. 1 data sheets =1 point v. 0 data sheets =0 points			
2	Track Record - three (3) contactable references (5 points per reference – a and b) And profile	(a) Contact Details = **3 points** (i) Company name = 1 (ii) Contact person = 1 (iii) Contact number = 1 (b) Relevant description of services = **2 points** (c) Organizational partnership and associations = **1 point**	16		
3	Staff experience and knowledge. 2 x staff CVs with relevant experience qualifications (8 points per resource)	Staff Security Experience = **3 points** (a) Staff experience 3 years or more = 3 (b) Staff experience 2 years = 2	14		

Phase 2 – Technical Evaluation Criteria Bidders must score a minimum of 75% (62/83) to proceed to the next evaluation phase					
	Description		**Weighted Score**	**Score**	**Comments**
		(c) Staff experience 1 year = 1 (d) Staff experience < 1 year = 0 Security Qualifications = **2 points** (e) Relevant qualification = 2 (f) No qualification = 0 Staff Networking Experience = **2 points** (g) Staff experience 3 years or more = 2 (h) Staff experience 1-3 years = 1 (i) Staff experience < 1 year = 0			
4	Project Plan and Project Governance	Project plan = **10 points** (a) Scope = 1 (b) Milestones = 2 (c) Risks = 2 (d) Deadlines / Duration = 2 (e) Dependencies = 2 (f) Project Governance Structure included = 1	10		
5	Incident Response Plan	Incident response plan = **5 points** (a) Call logging procedure = 1 (b) Call allocation/classification procedure = 2 (c) Escalation procedure = 2	5		
	Final Score		**83**		

Phase 3

Phase 3 - Evaluation Based on the 80/20 Preference Point System (PPPFA Scoring)
Only bids that comply with the requirements and conditions of the Auction and that meet the minimum criteria in the bid evaluation process as stipulated above will be considered for bid adjudication purposes. Adjudication of qualifying bids will be done in accordance with the 80/20 preference point system provided for in the Preferential Procurement Regulations, 2017. Pre-scoring of bids on the eProcurement system is illustrative only in respect of the potential outcome of the Auction and serves to enhance transparency in the bidding process as well as to encourage competitive bidding and B-BBEE compliance. Qualifying bids will be scored in the final PPPFA scoring to conclude the bid evaluation process and final price and total bid points may change accordingly. The ranking of the qualifying bids in terms of the scoring will be confirmed. The order of ranking of the qualifying bids will, however, remain the same since price, B-BBEE status levels and preference points claimed will not change once the Auction has closed.

Bid Evaluation Committee

	Name:	Signature:
1		
2		
3		
4		
5		