Eskom National Transmission Company South Africa ™	**SCOPE OF WORK - SPECIALISED TACTICAL RESPONSE SERVICES, SBI AND INVESTIGATION CONTRACT FOR NTCSA**	**NTCSA- Grids**

Title: Provision of Specialised Tactical Response Services, Security Business intelligence and Investigation as When required.

Document Identifier: **559-1167324521**

Alternative Reference Number: **N/A**

Area of Applicability: **NTCSA Grids**

Functional Area: **Security**

Revision: **0**

Total Pages: **38**

Next Review Date: **February 2031**

Disclosure Classification: **Controlled Disclosure**

Compiled by	**Functional Responsibility**	**Authorized by**
Christopher Nkosi	Melvin Murugen	Thomas Tshikalange
Snr Advisor Sec Ops	Middle Manager Sec Ops	Senior Manager Special Project Grids
Date: 16/10/2025	Date: 2025/10/20	Date: 20/10/2025

TABLE OF CONTENTS

1.1 Introduction

The National Transmission Company of South Africa (NTCSA) hereby invites qualified and experienced security service providers to tender for the provision of Outcome-Based Contracts (OBC) covering the following specialised services:

- Tactical response operations
- Security business intelligence
- Investigative services
- Integrated security systems and technology

These services are required at critical infrastructure sites, including:

- Central Grid
- East Grids
- Northeast Grid
- Southern Grids
- Northern Grids
- Western Grids
- Telecommunications Radio Sites

Note: These sites include National Key Points (NKPs).

These sites are of strategic importance to South Africa's national electricity grid. The tender aims to enhance security outcomes through a comprehensive turnkey solution that integrates advanced technology, Tactical response operations, Security business intelligence, Investigative services, Integrated security systems and technologies and measurable performance metrics. This integrated approach is designed to safeguard critical infrastructure, ensure operational continuity, and support national energy resilience.

The contract will be governed by Eskom's Outcome-Based Contracting model, which shifts focus from traditional input-based services to value driven, performance-based delivery. The successful bidder will be responsible for:

- Design, supply, installation, commissioning, and maintenance of an Integrated security (IACS) and other security technologies.
- Deployment of trained, PSIRA-compliant security personnel, aligned to site specific risk levels.
- Continuous monitoring and rapid armed response capabilities.
- Innovation and continuous improvement, including a technology roadmap and measurable cost-efficiency gains.
- Compliance with all legislative and regulatory frameworks, including the Critical Infrastructure Protection Act (Act 8 of 2019), MPSS, PSIRA, and Eskom's internal standards.

This contract will span 36 months, with all installed equipment and systems becoming the property of NTCSA upon installation. The service provider will be held fully accountable for all subcontractors and third-party vendors, with strict consequence management protocols in place for non-performance.

The overarching goal is to protect NTCSA's personnel, assets, information, and operations against evolving threats such as cable theft, vandalism, land invasion, and sabotage, while ensuring operational resilience and stakeholder confidence.

2. Supporting Clauses

2.1 Scope

2.1.1 Purpose

This document defines the scope of work for the provision of Tactical Response Operations, Security Business Intelligence, Investigative Services, and Integrated Security Systems and Technologies.

It supports the procurement of a 36-month Outcome-Based Contract (OBC) designed to deliver measurable, performance-driven protection outcomes through the integration of these services.

The contract is structured to:

- Enhance security resilience across NTCSA's strategic assets by integrating surveillance, access control, intrusion detection, and rapid response systems.
- Ensure full compliance with NTCSA's technical standards, the Critical Infrastructure Protection Act (Act 8 of 2019), PSIRA regulations, and Eskom's internal security specifications.
- Transfer ownership of all installed equipment, systems, and technologies to NTCSA upon installation, with a preference for high-specification solutions where feasible.
- Enable continuous improvement through innovation, data-driven performance monitoring, and a strategic reduction in reliance on manual guarding.

This scope of work serves as a foundational guide for service providers to deliver a turnkey, accountable, and future-ready security solution that safeguards NTCSA's personnel, infrastructure, and operations against evolving threats.

2.1.2 Objective

The objective of this scope of work is to establish a robust, integrated security framework for NTCSA's Central Grid, East Grids, Northeast Grid, Southern Grids, Northern Grids, Western Grids and Telecommunications Radio Sites through a 36-month Outcome-Based Contract (OBC).

This framework is designed to deliver measurable security outcomes, ensure compliance with national legislation, and safeguard critical infrastructure against evolving threats.

2.2 Recognition of National Key Point and Critical Infrastructure Status

NTCSA reaffirms its commitment to securing all grid infrastructure, including designated National Key Point areas, as part of South Africa's critical electricity transmission network.

2.3 Response to the Evolving Threat Landscape

Address the persistent and escalating threats posed by criminal activity, socio-economic instability, and political volatility. Specific risks include cable theft, equipment sabotage, land invasion, and malicious damage to property. The objective is to proactively mitigate these risks through specialised tactical response services, security business intelligence and investigations, technology-driven surveillance, rapid response capabilities, and community engagement.

- Rectify known weaknesses across the sites, including:
- Non-compliance of the substations and radio sites
- Absence of perimeter fencing and inadequate surveillance coverage.

2.4 Comprehensive Protection Scope

Ensure the protection of NTCSA's personnel, assets, information, and operational processes against current and emerging security threats. The solution must align with the findings of the Threat and Risk Assessment and support operational continuity across all facilities.

2.5 Legislative and Operational Compliance

Guarantee full compliance with all applicable laws and standards, including:

- Minimum Physical Security Standards (MPSS)
- Private Security Industry Regulation Act (PSIRA Act)
- Critical Infrastructure Protection Act 8 of 2019
- Eskom's internal security specifications and technical standards

2.6 Strategic Implementation via Outcome-Based Contracting

Deploy a performance driven OBC model that ensures accountability, innovation, and continuous improvement. The service provider must demonstrate full-time commitment, with active involvement from NTCSA's Threat and Risk Evaluation (TRE) team to monitor, evaluate, and enhance the security framework throughout the contract lifecycle.

2.7 Applicability

This document shall apply to NTCSA Grids.

2.8 Effective date

This document is effective from the date of signature.

2.9 Normative/Informative References

Parties using this document shall apply the most recent edition of the documents listed in the following paragraphs.

2.10 Normative

[1] ISO 9001 Quality Management Systems

[2] ISO 27000 Information Security Management Systems

[3] 240-86738968 – Specification for Integrated Security Alarm System for Protection of Eskom Installations and its Subsidiaries

[4] 240-78980848 – Specification for Non-Lethal Energised Perimeter Detection System (NLEPDS) for Protection of Eskom Installations and its Subsidiaries

[5] 240-91190304 – Specification for CCTV Surveillance with Intruder Detection

[6] 240-102220945 – Specification for Integrated Access Control System (IACS) for Eskom Sites

[7] 240-170000098 – Security Public Address System for Substations and Telecoms High Sites

[8] 240-139282493 – Security Lighting for Eskom Applications

[9] Minimum Information Security Standards (MISS), 1996

[10] National Key Points Act 102 of 1980

[11] Critical Infrastructure Protection Act 8 of 2019

[12] Constitution of the Republic of South Africa Act 108 of 1996

[13] Occupational Health and Safety Act 85 of 1993

[14] Private Security Industry Regulation Act 56 of 2001

[15] Protection of Personal Information Act 4 of 2013

2.11 Informative

[1] 32-86: Integrated Risk Management Policy

[2] 32-84: Security Management Policy

[3] 32-727: Safety, Health, Environment, and Quality Policy

[4] 32-85: Information Security Policy

[5] 240-53716911: Overarching Group Information Technology (IT) Policy

[6] 238-14: Physical Protection Measures for Nuclear Power Stations and Facilities

[7] GSR (Government Security Regulator) Minimum Physical Security Standards (MPSS)

2.12 Definitions

Definition	Explanation
Tender	Refers to an open or closed competitive request for quotations / prices against a clearly defined scope / specification.
Integrated Access Control System	It is an electronic system that aims to collaborate and align efforts across the logical and physical security domains to standardise access control within Eskom.
Control Centre	Where alarms and CCTV footage are monitored and needed response/s initiated from. The alarms and CCTV footage can be aggregated to a national security control centre that can initiate requisite actions from a national perspective.

2.13 Abbreviations

Abbreviation	Explanation
OBC	Outcome-Based Contract
CCTV	Closed Circuit Television
KPI	Key Performance Indicator
NTCSA	National Transmission Company of South Africa
SSP	Security Solutions Physical
SACAA	South African Civil Aviation Authority
TRT	Tactical Response Team
SBI	Security Business Intelligence
COIDA	Compensation for Occupational Injuries and Disease Act
PSIRA	Private Security Industry Regulation Act
ROI	Return on Investment
PAPAA	Performing Animal Protection Amendment Act

2.14 Roles and Responsibilities

2.15 2.5.1. Role of the employer

a) Detailed Standard Operating Procedures. Procedures will be provided by the Employer.

2.16 Contractor responsibilities

To ensure the delivery of high-quality, compliant, and accountable security services, the appointed contractor must meet the following minimum requirements.

2.17 RESPONSIBILITIES OF THE CONTRACTOR SECURITY SITE REPRESENTATIVE

2.18 Legal and Regulatory Compliance

- The contractor must be a legally constituted entity authorized to provide security services within South Africa.
- The contractor must hold a valid registration with the Private Security Industry Regulatory Authority (PSIRA).
- All deployed security personnel must be PSIRA-registered and carry valid proof of registration while on duty.
- The contractor must possess valid firearm licenses for all weapons used on site, in accordance with the Firearms Control Act.
- All wages and salaries paid to security personnel must comply with the Wage Determination Act and relevant labour legislation.

2.19 Operational Infrastructure

A fully equipped 24/7 Control Room must be maintained by the contractor, capable of real-time monitoring, communication, and incident coordination.

- All communications between the control room and site personnel must be accurately logged in an Occurrence Book (OB), including timestamps, nature of communication, and actions taken.
- In the event of a security incident, Security contractor must immediately notify control room, and record the incident in the OB.
- The control room must promptly inform the NTCSA Protective Services Representative and Site Owner of any incident.
- Each site must maintain uninterrupted 24-hour communication with the control room via contractor-supplied radio or cellular devices.
- The service provider may propose equivalent electronic system to ensure that we eliminate the manual process.

2.20 Incident Management and Reporting

- Intelligence Investigators as when required must respond to reported incidents within 2 hours.
- A preliminary report must be submitted to NTCSA within 24 hours.
- A final investigation report must be submitted within 7 days, or weekly progress updates if the investigation is ongoing.

2.21 Personnel Appearance and Equipment

- All TRT must wear a standardized, professional security uniform, including weather-appropriate PPE (e.g., raincoats, warm jackets).
- TRT must be equipped with essential tools such as batons, torches, and handcuffs.

2.22 Site-Specific Preparedness

- A Security Threat Assessment and Site-Specific Work Instruction must be jointly developed by the contractor, NTCSA Site Owner, and Security Services Representative.
- All contractor staff deployment must be trained and fully conversant with the Work Instruction applicable to their assigned site.
- Each site must maintain a clean, organized Occurrence Book for daily activity and incident logging.
- All activities must be accurately recorded by the on-duty contractor staff.
- A Visitors Register must be maintained at each site, provided by NTCSA, and completed diligently by the contractor deployed staff.
- It is the responsibility of the security officer to ensure all registers are correctly and legibly completed.

2.23 Logistics and Engagement

- NTCSA will not provide accommodation for contractor staff; this remains the sole responsibility of the contractor.
- Contractor supervisory and managerial staff must attend monthly NTCSA planning meetings at designated venues or via Ms team.

- The contractor must comply with the Occupational Health and Safety Act and be briefed on all NTCSA standards and procedures.

2.24 Technology Implementation

- The contractor is responsible for the deployment, integration, and maintenance of all security technologies installed under this contract, ensuring full functionality and compliance with NTCSA specifications.

2.25 Process for Monitoring

To ensure consistent delivery of high-quality security services, the contractor shall implement a structured process monitoring framework aligned with NTCSA's operational standards and Eskom's Outcome-Based Contracting (OBC) model.

This includes daily operational oversight, real-time incident tracking, and performance evaluation against predefined Key Performance Indicators (KPIs).

Monitoring will be conducted through a centralized control room with 24/7 surveillance and communication capabilities, supported by automated system health checks and manual inspections.

Regular performance reviews, monthly compliance audits, and ad hoc evaluations will be conducted by NTCSA's Threat and Risk Evaluation (TRE) team to assess service effectiveness, identify gaps, and drive continuous improvement.

All incidents, faults, and deviations must be logged, investigated, and resolved within stipulated timeframes, with detailed reporting submitted to NTCSA for verification and accountability.

2.26 Related/Supporting Documents

559-348635181 OBC Guidelines.

2.27 Request for proposal

3.1 Project scope

The National Transmission Company of South Africa (NTCSA), Special Project Grids is inviting proposals from qualified and experienced security service providers to deliver comprehensive, specialised tactical response services, security business intelligence and investigations, technology-driven surveillance, rapid response capabilities, and community engagement. These sites include both National Key Point (NKP) and critical infrastructure (Line &Servitudes , Substations & Telecommunication Radio sites), requiring tailored security interventions aligned to their respective risk profiles.

The successful bidder(s) will be expected as when required to design and implement a turnkey security solution that incorporates specialised tactical response services, security business intelligence and investigations, technology-driven surveillance, and measurable performance outcomes. Service delivery must be structured around the defined risk levels applicable to each site within all the NTCSA grids, ensuring that protection measures are proportionate, responsive, and compliant with NTCSA's operational standards and legislative obligations.

3.2 Scope and Risk Levels

This engagement encompasses seven strategically important facilities: Central Grid, East Grid Northeast Grid, Southern Grid, Northern Grid, Western Grid, Telecommunications Radio Sites

Note: These sites include National Key Points (NKPs).

Each site has been assessed and categorized according to its risk level, which informs the minimum-security requirements and operational expectations. The scope of work addresses three distinct risk categories, ensuring that security measures are proportionate to the threat profile and operational criticality of each facility.

Risk Level	Sites	Minimum Security Standards
Risk Level 2 – Medium to High Risk	• East Grids • Southern Grids • Western Grids	**Security Objective**: Prevent unauthorized access, deter criminal activity, and enable swift, coordinated response to incidents. **Minimum Requirements**:

		• **Comprehensive CCTV Surveillance**: High-definition cameras with intelligent analytics (e.g., motion detection, loitering alerts) covering all critical zones. • **Advanced Integrated Alarm Systems**: Multi-layered sensors (perimeter, vibration, volumetric) linked to CCTV and access control systems. • **Integrated Access Control**: Card and biometric access at all entry/exit points, with audit trails and remote management capabilities. • **24/7 Centralised Monitoring**: Dedicated control room operators for continuous oversight, alarm verification, and dispatch coordination. • **Rapid Armed Response**: Priority response with defined SLAs, pre-identified access routes, and site familiarization protocols. • **On-Site Deterrence**: Uniformed, PSIRA-registered C-grade security guards (armed or with escalation protocols) focused on access control and visual deterrence during high-risk periods. Engagement is supported by technology and armed response units.
Level 3 (High Risk)	• Central Grids • Northeast grids • Telecommunications Radio Site	**Security Objective**: Maximize prevention of sophisticated attacks, ensure immediate detection, and enable overwhelming response to protect critical assets. **Minimum Requirements**: • **AI-Powered Advanced Surveillance**: High-definition cameras with AI analytics for anomaly detection, facial recognition (where permissible), object tracking, and predictive threat analysis. Integrated with Public Address (PA) systems for real-time audio alerts. • **Multi-Layered Perimeter Defence**: Fibre optic fencing, ground radar, and thermal imaging sensors, combined with physical hardening measures. • **Robust Integrated Access Control**: Biometric systems with anti-passback functionality and comprehensive visitor management. • **24/7 Dedicated Monitoring & Intelligence**: Proactive monitoring by highly trained operators using business intelligence feeds for pre-emptive threat identification and response. • **Immediate Armed Response**: Direct deployment of armed response teams with the shortest possible SLAs, including dedicated on-call units or co-location agreements. • **Highly Trained On-Site Security Guards (Armed Recommended)**: Visible, well-equipped personnel trained for rapid response and coordination with external armed units. Patrols must be intelligence-driven and aligned with site-specific threat profiles.

3.2.1 Scope of Work

These services required shall, any time be expected to include, but not limited to the following:

3.3 Preliminaries and Generals

- Comply with SHEQ such as Medicals (Entry, Periodic and Exit) PPE etc (Contractor to Provide Breakdown of Cost)

3.4 Air surveillance , Physical Integrated security Systems

Key Components:

- Deployment of UAVs/Drones: Equipped with high-resolution cameras, thermal imaging, and GPS tracking.
- Flight Planning & Operations: Scheduled patrols and on-demand surveillance missions.
- Real-Time Monitoring: Live video feeds to centralized control rooms.
- Data Storage & Analysis: Secure archiving of surveillance footage and integration with analytics platforms.
- Compliance & Licensing: Adherence to aviation regulations and airspace permissions.
- Maintenance & Support: Regular servicing of aerial equipment and software updates.

3.5 Physical Integrated Security Systems

To ensure the protection of NTCSA's critical infrastructure, personnel, and operations, the appointed service provider must deliver a comprehensive, integrated physical security solution tailored to site-specific risk levels and operational requirements. This solution must combine skilled personnel, advanced security technologies, and a strategic roadmap for continuous improvement.

Core Systems:

- Perimeter Intrusion Detection Systems (PIDS):
  - Sensors, fiber optics, and radar to detect unauthorized access.
  - Real-time alerts and automated response protocols.
- Access Control Systems (ACS):
  - Biometric authentication, RFID cards, and smart locks.
  - Centralized management of personnel access rights.
- Closed-Circuit Television (CCTV):
  - High-definition cameras with night vision and motion detection.
  - AI-powered video analytics for threat detection and incident review.
- Alarm & Panic Systems:
  - Emergency buttons and automated alerts to security teams.
  - Integration with public address systems for evacuation protocols.
- Physical Security Information Management (PSIM):
  - Unified dashboard for monitoring all subsystems.
  - Incident logging, reporting, and escalation workflows.

3.6 Technology Roadmap and Innovation Strategy

The service provider must submit and implement a Technology Roadmap that outlines how innovative solutions will be introduced, scaled, and maintained over the contract period. This roadmap must demonstrate alignment with Eskom's OBC principles and include:

Phase 1: Baseline Deployment

- Installation of CCTV, access control, alarm systems, and intrusion detection
- Commissioning of centralized monitoring infrastructure
- Integration of legacy systems into a unified platform

Phase 2: Optimization and Automation

- Deployment of AI-powered analytics for surveillance and threat detection
- Reduction of manual guarding through technology substitution
- Implementation of predictive maintenance and automated fault alerts

Phase 3: Innovation and Scalability

- Introduction of advanced technologies (e.g., drones, thermal imaging, fibre optic sensors)
- Expansion of systems to additional NTCSA sites or zones
- Continuous improvement through quarterly performance reviews and stakeholder feedback

Phase 4: Knowledge Transfer and Sustainability

- Training NTCSA personnel on system operation and basic maintenance
- Full documentation of system architecture, SOPs, and emergency protocols
- Handover of all data, licenses, and assets at contract conclusion

Expected Outcomes:

- 30–40% reduction in guard force by Year 3 through technology integration
- Improved incident detection and response rates
- Demonstrable cost savings and operational efficiency
- Full compliance with Eskom's technical specifications and innovation benchmarks

3.7 Project Deliverables:

- Site assessment and risk analysis.

- Design, supply, installation, and commissioning of systems.
- Decommissioning of outdated infrastructure.
- User training and documentation.
- Ongoing maintenance and technical support

3.8 Business intelligence to prevent petty and organised crime

- Research/investigations of the metal market and recycling industry in South Africa to determine the destination of stolen NTCSA equipment.
- Provide systems product which enable the collection, reception, recording, storage, use and dissemination. E.g., this includes computerised systems that contain crime records, open sources data, information files, analysis tool, specialised database and case management tool.
- Provision of access to facilities or system for acquisition of new information and SBI gathering to determine identified needs.
- The profiling of criminal syndicates and unscrupulous scrap metal dealers.
- Profiling offenders not related to criminal syndicates within communities involved with theft of NTCSA Network Infrastructure.
- The use of whistleblowers within the communities involved with the theft of NTCSA Network Infrastructure.
- Policing of the Provincial Disposal Contract/ensure effective control of NTCSA material and equipment through appropriate commercial procedures.
- Investigate criminal activities committed by metal merchants, smelters, exporters, metallurgical laboratories, relating to the trading, transporting, or managing of stolen NTCSA equipment.
- Investigate NTCSA internal misconducts and criminal activities committed by employees and contractors, as and when reported.
- Provide written progress report on the investigation to the responsible NTCSA Line Manager/Requestor.
- Compile a comprehensive investigation report with detailed findings and recommendations for action/implementation by NTCSA.
- Research/investigations into the activities of criminal elements and crime syndicates targeting NTCSA infrastructure.
- NTCSA network infrastructure by means of obtaining SBI and putting an end to these crimes and identifying criminals for prosecution.

- NTCSA material identification statements in support of criminal investigations and prosecution upon recovery.
- Interact with law enforcement agencies to provide training were identified and to create awareness on the impact of the crime.
- Interaction with the judiciary to provide training and support where required.
- Develop appropriate technology solutions in support of this strategy.
- Identify hotspots where equipment theft syndicates and petty offenders who are not syndicates, are operating and initiate SBI driven operations to apprehend them.
- Attend and participate at SAPS disruptive operations in various areas.
- Compile and maintain case dockets with sufficient evidence to apprehend and initiate prosecution, or to take other necessary action against the above.
- Submit processed evidence to relevant government authorities for appropriate action.
- Monitor and support relevant government authorities during above-mentioned action.
- Maintain a database to record all information gathered during the research/investigations.
- Provide NTCSA with SBI which may be used to establish an in-house active crime – SBI capability.
- Establish measures to counter act the prevalence of corruption in relation to crimes of this nature.
- The service provider shall have an existing electronic database of the criminals, suspects, syndicates, groups, assets recovered, arrests, and convictions.
- The service provider will supply a dual server that can be housed in a safe location decided by NTCSA to enable NTCSA to access the data without delays. Access levels to the electronic database will be decide on and managed by NTCSA Grid Security Manager.
- Provide NTCSA with access to content – e.g., Read/View rights on incident management system / existing database containing syndicates, suspects, scrap Dealers, NTCSA Hot spots and modus operandi of suspects.
- The service provider shall have an air surveillance capability fitted with night vision – preferably doing so by using drones, mainly for overhead lines and in mountainous areas.
- The service provider is to furnish NTCSA with electronic backups of all data gathered on monthly basis.
- The service provider shall have at least 5 years of provable experience of investigating and or dealing with non-ferrous infrastructure vandalism and thefts.

- The service provider should have a legal team at their disposal experienced in criminal law with a particular focus on network infrastructure crime and criminal matters amendment act. The team must have the ability to initiate court proceedings, both civil and criminal and must be able to assist in the recovery of proceeds of crime with the assistance of Asset Forfeiture Unit.
- Monitor and investigate illegal exports of non-ferrous metals at all ports of exits.
- Monitor the syndicate members after their release from prison.
- The service provider must support the criminal justice system during the criminal prosecution process, and function as a custodian in criminal cases on behalf of NTCSA. They must be able to give sound advice to National Prosecuting Authority and SAPS concerning the best cause of action in the matters.
- The service provider will arrange for the centralisation of criminal cases from various areas with the assistance of the NPA and SAPS to ensure the most effective way of prosecuting criminals.
- The service provider must conduct syndicate mapping and evidence analysis.
- Identify and Profile offenders/syndicates of Network Infrastructure Crime
- Identify Crime Hotspots/Risk Areas where infrastructure crime syndicates are operating.
- Identify the Modus Operandi and specific targets, sites, areas (Geographical info)
- Provide reports on investigation activities, performance, and successes.
- Conduct and provide Root cause analysis.
- Provide and quantify the losses (including consequential losses) – rand value estimates.
- Conduct SBI driven/disruptive operations – minimum >20 per month.
- Have a well-established and managed Informer network.
- Conduct Covert operations / infiltration by possessing all the necessary resources – people, tools and technology etc.
- Shall arrange and participate in conducting entrapment (Section 252A)
- Be able to track/trace profile and establish ownership, e.g., suspected vehicles, telephone numbers, etc.
- Service on and as requested by NTCSA (Ad-hoc/specific): e.g., deeds, company information, individual information, criminal records, verification of documentation regarding identification/certifications/registrations etc.
- Social media network monitoring for security threats against NTCSA network infrastructure i.e., overhead, underground lines, substations and other critical infrastructure in the Grid.

- Transfer of skill, investigation information and workplace experience to NTCSA security teams must be conducted by service provider.
- At the end of the contract – NTCSA IP to be handed back to NTCSA Security Contract Service
- Manager (Corporate memory to be with NTCSA) within 30 calendar days.
- Form Part of disruptive Operations with various law enforcement agencies within the Grid , provide report of outcomes of each operation including any successes.
- Targeted Patrols (in hotspot areas)
- Opening of cases with SAPS, completing of dockets on behalf of NTCSA
- Testifying in courts
- Apprehend offenders.
- Networking with relevant stakeholders including farming forums and other neighbourhood security clusters.
- Technology shall be deployed in identified hotpots areas as tasked by the contract service manager.
- The technology must be able to delay, deter and detect and send alerts on real time to be able to effect arrests.
- The service provider shall offer a comprehensive range of polygraph services when offenders are suspected of being complicit to any crime affecting NTCSA.

3.9 Tactical Response Team (TRT)

- Tactical support and security services to be rendered shall be crime prevention and crowd disruption focused for purposes of monitoring and safeguarding the identified Grids high risk and vulnerable areas within the NTCSA.
- Armed escorting of personnel critical deliveries of commodities to and from sites, as and when required.
- The protective condition shall focus on deterring, detecting, deflecting and defending against acts of criminality and economic sabotage such as disruption & obstruction of access / egress routes at the substations , critical infrastructure tampering, vandalism, unauthorised access, unauthorised removal of copper cables, other assets and equipment, bypassing security measures, security breaches, security incidents, industrial action (strikes, demonstrations, protests, sit-ins, picketing etc.), but not limited thereto.

- The deployed TRTs shall be agile, swift, observant and vigilant; and shall rapidly respond to alarms, security incidents, crime scenes, imminent or potential threats in the substations environment and that may negatively affect security of supply or introduce risks to operational performance and stability at the Substations .
- Use shall be made of overt and covert deployment of TRTs as and when required.
- Tactical deployed officers are to be equipped with body cams to support the monitoring of tasks and incident investigation aspects, internal and external to the substations. Foot and vehicle patrols shall be conducted to cover the targeted substations high risk and critical vulnerable areas and shall not be predictable.
- Reaction and response to any security emergencies or life-threatening situations on site without delay.
- Prevention of unauthorised removal of NTCSA assets from substations sites and network infrastructure, through searches and screening of people, objects, vessels and vehicles.
- Provide situational and operational reporting on issues and incidents.
- Record events and incidents through audio- visual or digital means e.g. strike actions, protests, gatherings, demonstrations, crime scenes, but not limited thereto.
- Perform crime scene management and preservation of evidence, witnesses, etc. until SAPS responds and takes over.
- Provide K9 security services

3.10 Body-Worn Camera Integration and Armed response

As part of Eskom's commitment to operational transparency, incident accountability, and evidence-based response management, Body-Worn Cameras (Bodycams) shall be included as a mandatory component of the standard uniform for all TRT and deployed under the Independent Armed Response Service.

Minimum Operating Standards for Bodycams:

- **Deployment Requirement**:
  - All TRT must wear an operational body-worn camera during active-duty hours, including during patrols, incident response, and site engagements.
- **Recording Protocols**:

- Cameras must record continuously while on duty.
- Footage must be securely stored and retained according to Eskom retention policy.
- Any incident-related footage must be flagged and archived for investigative and legal purposes.

- **Data Access & Management**:
  - Only authorized personnel may access recorded footage.
  - All footage must be encrypted and stored in compliance with POPIA and other applicable data protection regulations.
  - Service providers must maintain a secure digital evidence management system.
- **Incident Review & Audit**:
  - Bodycam footage will be used to verify incident reports, assess officer conduct, and support forensic investigations.
  - Eskom reserves the right to request footage for random audits, disciplinary reviews, or legal proceedings.
- **Training & Compliance**:
  - All officers must be trained in the proper use, handling, and maintenance of bodycams.
  - Officers must acknowledge and comply with Eskom's bodycam usage policy prior to deployment.
- **Failure to Comply**
  - Non-compliance with bodycam protocols may result in disciplinary action, removal from duty, or contract penalties.

3.11 FIREARMS

Only NTCSA approved firearms are allowed.

For the usage in terms of this contract licensed 9mm pistols for self-defence and shotguns with rubber bullets will be applicable. Armed Security officers must have South African Police competency certificates for the specific firearm in possession thereof.

The contractor is responsible for providing firearms, ammunition, belt / shotgun slings, holsters, tactical torches, pepper spray, firearm safes, crowd control equipment, registers as per the Firearm Control Act, for the management and control of the company's firearms.

No TRT's shall be permitted to use or be issued with an NTCSA firearm under any circumstances.

Safe handling of firearms during shift changes must be always adhered to. The contractor must ensure that a procedure is put in place to that effect.

Safes must be provided by the contractor for the safekeeping of firearms not in use.

The contractor must ensure provision of equipment/facilities for making firearms safe. A procedure to that effect, should also be in place.

The contractor must ensure that Security officer's private firearms are not utilized for their business purposes, in terms of this contract.

No Contractor firearms will be kept safe / stored on Grids premises; the company is to ensure that the firearms are issued / returned / stored & transported in terms of the Provision of the Firearm Control Act.

3.12 SUPERVISION AND CONTROL

- All deployed guards must be supervised by a duly assigned and delegated PSIRA Grade B supervisor per shift.
- The supervisors must ensure that TRT's are assisted to reach the sites and paraded when reporting on and off duty.
- The posting of TRTs is required to be done by the Supervisor at all sites (the practice of "self-posting" is not permitted).

3.13 REPORTING AND COMMUNICATION

- The Contractor must ensure suitable continuous communication between the operational control room and their deployed staff. Either one or more of the following mediums of communications shall be provided as per user requirements: hand-held

radios, satellite radio, contracted cell phones, base radios and push to talk (PTT).

- An operational centre / control room shall remain in constant reach and communication with the deployed security personnel, at all sites.
- Situational reports and a complete operational report - Daily briefings and debriefings on location (issuing of tasks).
- A WhatsApp communication platform will be established by the Grids Security Manager with all Team Leaders / Operations managers responsible for the Various Grids.

3.14 BUSINESS CONTINUITY MANAGEMENT AND CONTINGENCY PLANS

The Contractor must have contingency plans in place for the following:

- Own Strike/Labour unrest amongst own staff.
- Shortage of Manpower due to e.g., absenteeism, sick leave annual leave.
- Equipment Failure e.g., Vehicle breakdown and Communication system.
- Internal grievance procedures.

3.15 INCIDENT REPORTING AND INVESTIGATION

- All incidents and response to incidents must be managed according to the relevant SOPS and/or work instructions for each site.
- All incidents and response/s must be immediately reported to the NTCSA control room.
- The SAPS must be contacted immediately only for criminal incidents or suspected ongoing criminal activities, including firearm related incidents e.g. accidental discharge of firearm
- Weekly status reports are to be supplied by the Contractor.
- The contractor is to ensure that all involved personnel are available for relevant court proceedings, incident investigations and assist NTCSA and the SAPS in their investigations as and when required.

All incidents (including incidents in terms of the Occupational Health and Safety Act), should be

reported within 24 hours and a preliminary investigation report provided.

TRT equipped with:

- Standard PPE (raincoats, warm jackets, reflective gear)
- Body-worn cameras (compliant with Eskom standards)
- Operational tools (batons, torches, handcuffs)
- Site-specific induction and training

3.16 Security Screening Requirements of TRT

The supplier shall provide to the designated NTCSA contracts manager, the following:

- Results of Criminal background checks of the TRT not older than 3 months from the date of deployment.
- The report shall be provided within fourteen days from date of deployment.
- All Security officers must be registered with PSIRA at the required grade.
- Tactical security officers Grade C with Armed response and or Cash in Transit. Where the PSIRA certificate does not indicate as such proof of course results for Armed response, Cash in Transit, Crowd management to accompany the PSIRA certificates.
- All supervisors should have a PSIRA Grade B and all team leaders a minimum of Grade A.
- Proof of Tactical security training and experience of all deployed officers at site level, including crowd control.
- Armed Security officers must have completed SASSETA training on the specific firearms they are expected to use.
- Armed Security officers must possess valid firearm competency certificates for business purposes (issued by SAPS) and always carry it.
- Armed security officers should have undergone Regulation 21 training during 2025/2026 FY.
- Security officers will be expected to sign a declaration of Secrecy before commencement of their duties in terms of this contract.
- Copies of signed PSIRA Code of Conduct of all Security Officers deployed at sites.

3.17 Patrol and Perimeter Services

Conduct scheduled and intelligence-driven patrols across all designated zones, including:

- Perimeter fencing, high-value asset areas, and vulnerable locations
- Use of mobile technology for GPS-tracked patrol logging
- Real-time reporting of anomalies or breaches
- Integration with AI analytics to optimize patrol routes and frequency

3.18 Incident Response

As when required provide 24/7 rapid armed response capability to all verified security alerts and emergencies. Response protocols must include:

- SLA compliance: ≤15 minutes (urban), ≤30 minutes (remote)
- Coordination with control room operators and law enforcement
- Scene preservation and evidence handling procedures
- Real-time incident escalation and reporting via secure digital platforms

3.19 Emergency Management

Maintain full operational readiness for a range of emergency scenarios, including:

- Sabotage, fire, land invasion, civil unrest, and infrastructure tampering
- Trained personnel in evacuation, containment, and first-response protocols
- Integration with NTCSA's emergency communication systems
- Post-incident investigation and root cause analysis reporting

3.20 Community Involvement

- **Community Liaison:** Develop and implement a strategy for effective and positive engagement with local communities surrounding the protected sites. This should include regular communication channels, awareness campaigns about the importance of electricity infrastructure, and mechanisms for receiving community intelligence regarding suspicious activities.

- **Job Creation/Local Procurement:** Where feasible and in line with NTCSA's procurement policies, outline strategies for local job creation, skills transfer, and procurement from local

businesses within the seven facilities or grids, contributing to community upliftment and fostering positive relationships.

- **Collaborative Safety Initiatives:** Propose and participate in joint safety awareness initiatives with local community structures, emphasizing the dangers of illegal connections and infrastructure tampering.

3.21 Liaison with Law Enforcement Agencies

- **Formal Communication Protocols:** Establish and maintain formal, documented communication protocols with the South African Police Service (SAPS) units operating in seven facilities or grids, including relevant specialized units (e.g., Non-Ferrous Metals Combating Unit, Public Order Policing).
- **Intelligence Sharing:** Develop mechanisms for secure and timely sharing of intelligence regarding criminal activities, modus operandi, and identified hotspots with SAPS and other relevant law enforcement agencies.
- **Joint Operations and Response:** Demonstrate a proven capability and willingness to participate in planned joint operations with SAPS and other security forces.
- **Evidence Collection and Preservation**: Ensure all security personnel are trained in proper scene preservation and evidence collection techniques to support SAPS investigations and improve the chances of successful arrests and prosecutions. Provide detailed incident reports that meet legal evidentiary standards.
- **Reporting and Compliance:** Adhere strictly to all legal requirements for reporting criminal incidents and cooperates fully with law enforcement in their investigations.

3.22 Handover Phase (At Contract End or Termination):

To ensure continuity, transparency, and operational readiness at the conclusion or transition of the contract, the appointed service provider must deliver a comprehensive handover package and facilitate full knowledge transfer. This includes technical documentation, training, licensing, and asset management, whether the Security Control Centre (SCC) is being handed over to NTCSA or decommissioned.

3.23 As-Built Documentation

Provide complete and accurate documentation for the SCC infrastructure, including:

- Architectural, electrical, and network diagrams detailing system layout and connectivity.
- Equipment manuals, warranties, and licensing agreements for all installed hardware and software.
- Software configurations, administrative guides, and user manuals for all integrated systems.
- Standard Operating Procedures (SOPs), training materials, and emergency protocols used during the contract period.
- Historical data archives, including incident logs, system performance reports, and maintenance records.

3.24 Training

Deliver comprehensive training to NTCSA's nominated personnel (or a successor service provider's team) covering:

- Full operation and administration of SCC systems
- Basic troubleshooting and maintenance procedures
- Emergency response protocols and escalation procedures

3.25 Knowledge Transfer

Facilitate structured knowledge transfer sessions to ensure continuity of operations. This must include:

- Operational procedures and workflows
- Threat landscape insights and site-specific risk profiles
- Key stakeholder contacts and escalation paths
- Status of ongoing projects, upgrades, or unresolved issues

3.26 Licensing and Ownership Transfer

Support NTCSA in the seamless transfer of:

- All software licenses, service agreements, and warranties
- Access credentials, encryption keys, and system rights

- Ownership of all installed technologies and data assets

3.27 Physical Asset Handover

Securely hand over all physical assets related to the SCC, including:

- Keys, access cards, biometric credentials
- Hardware components, backup devices, and mobile units
- Inventory lists and condition reports

3.28 Decommissioning (If Applicable)

If the SCC is to be decommissioned, the contractor must provide a detailed plan that ensures:

- Secure and environmentally responsible disposal of hardware and materials
- Data sanitization and destruction in compliance with POPIA and NTCSA standards
- Final audit and verification of decommissioning activities
- Closure report summarizing all actions taken and residual risks (if any)

3.29 Key performance indicators (KPI'S)

The performance of the appointed service provider will be rigorously monitored and evaluated against a comprehensive set of Outcome-Based Key Performance Indicators (KPIs). These KPIs are designed to ensure measurable improvements in security outcomes, operational efficiency, regulatory compliance, and innovation across NTCSA's critical infrastructure.

Primary KPIs: Investigations & Intelligence Gathering

KPI	Target	Measurement Method	Reporting Frequency
1. Number of investigations initiated monthly	≥ 30	Number of investigations initiated per month. 7 days preliminary investigation report. If its ongoing investigation within a month or court investigation ongoing until concluded.	Every 2 weeks report. Investigation reporting Monthly.

2. Percentage of investigations resulting in actionable intelligence	≥ 80%	Percentage of investigations resulting in actionable intelligence	Include in monthly progress report to NTCSA Head of Security Manager, with breakdown by Grids , type of crime, and syndicate involvement.
3. Number of SBI-driven disruptive operations	≥15/month	Number of SBI-driven disruptive operations conducted (15 minimum 15/month)	Monthly operational performance report with: • Date and location of each operation • Type of disruption • Syndicate or offender targeted • Outcome and follow-up actions
4. Number of site surveillance	≥50/month	Site surveillance reports	Monthly
5. Number of root cause analyses completed	≥ 5/month	Root cause analyses conducted per quarter	Weekly and consolidated monthly strategic intelligence report, detailing: • Incident overview and context • Identified root causes (technical, procedural, human, systemic) • Recommendations for mitigation or prevention • Linkage to broader crime trends or syndicate activity
6. Number of crime hotspots identified and mapped	≥ 1/month	Number of hotspots identified and mapped Number of syndicate mapping and evidence analysis reports completed	Monthly intelligence report with: • Location coordinates and description • Type of criminal activity observed • Associated syndicates or offenders

			• Visual maps and overlays (if applicable) • Recommendations for surveillance or intervention • Geo - spatial analysis reports

KPIs: Case Management & Legal Support

KPI	Target	Measurement Method	Reporting Frequency
1.Progress reports submitted on time	100% compliance	Progress reports submitted on time	Every 2 weeks progress report
2.Comprehensive investigation reports delivered	= 1/Month	Comprehensive investigation reports delivered	1 month
3.Case dockets compiled with sufficient evidence	≥ 90% of cases	Case dockets compiled with sufficient evidence	1 month
4.Number of cases opened with SAPS	≥ 30/month	Number of cases opened with SAPS	Daily
5.Court testimonies provided	As required by NTCSA	Court testimonies provided	Daily

KPIs: Strategic Intelligence & Technology Deployment

KPI	Target	Measurement Method	Reporting Frequency

1.Technology deployed in hotspot areas	100% of identified hotspots	Technology deployed in hotspot areas	As and when required based on intrusion
2.Real-time alerts generated and responded to	≥ 95% within SLA	Real-time alerts generated and responded to	Daily
3.Surveillance missions conducted (drone/night vision)	≥ 10/month	Surveillance missions conducted (drone/night vision)	Daily
4.Number of successful apprehensions due to tech-enabled detection	≥ 5/month	Number of successful apprehensions due to tech-enabled detection	Daily
5.Number of polygraph tests conducted	As requested by NTCSA	Number of polygraph tests conducted	As requested by NTCSA

KPIs: Data Systems & Infrastructure

KPI	Target	Measurement Method	Reporting Frequency
1.Monthly electronic backups submitted	100% compliance	Monthly electronic backups submitted	Every 2 week
2.Database update frequency	100 compliances	Database update frequency	Daily
3.Dual server uptime and accessibility	≥ 99.9%	Dual server uptime and accessibility	Daily
4.Access rights managed by NTCSA Grid Security Manager	100% compliance	Access rights managed by NTCSA Grid Security Manager	As when required

KPIs: Covert Operations & Whistle-blower Network

KPI	Target	Measurement Method	Reporting Frequency
1.Covert operations conducted	≥4/month	Covert operations conducted reports	Weekly
2.Whistleblower leads verified and acted upon	≥5/month	Whistleblower leads verified and acted upon	Monthly

KPIs: Social Media & Threat Monitoring

KPI	Target	Measurement Method	Reporting Frequency
1.Credible threats identified via social media	100% Compliance	Credible threats identified via social media	Daily
2.Response time to social media alerts	≤ 24 hours	Response time to social media alerts	Immediately
3.Incidents prevented due to early detection	≥ 30/month	Incidents prevented due to early detection	Weekly and consolidated monthly

KPIs: Training & Knowledge Transfer

KPI	Target	Measurement Method	Reporting Frequency
1.Training sessions provided to NTCSA teams	As and when required	Training sessions provided to NTCSA teams	As and when required.
2.Skill transfer reports submitted	As and when required	Skill transfer reports submitted	As and when required
3.Percentage of NTCSA staff trained	≥ 80% of security team	Percentage of NTCSA staff trained	As and when required

KPIs: Stakeholder Engagement & Collaboration

KPI	Target	Measurement Method	Reporting Frequency
1.Engagements with farming forums/security clusters	≥ 5/quarter	Engagements with farming forums/security clusters	Quarterly
2.Participation in SAPS disruptive operations	≥ 20/month	Participation in SAPS disruptive operations	Daily and Monthly consolidated report
3.Feedback score from NTCSA and stakeholders	≥ 90% satisfaction	Feedback score from NTCSA and stakeholders	Monthly

KPIs: Contractual Compliance & Handover

KPI	Target	Measurement Method	Reporting Frequency
1.NTCSA IP and corporate memory handed over	Within 30 days post-contract	NTCSA IP and corporate memory handed over	Within 30 days post-contract
2.Compliance with SLA terms and deliverables	100% compliance	Compliance with SLA terms and deliverables	Monthly
3.Audit score on data integrity and security	≥ 95%	Audit score on data integrity and security	Monthly

These KPIs form the foundation of NTCSA's performance management framework and will be used to determine service provider accountability, payment eligibility, and contract continuation. Failure to meet targets will trigger Eskom's Consequence Management Framework, including financial penalties, retraining, and potential contract termination.

Primary KPIs: Operational Excellence and Service Reliability

These KPIs support the core security outcomes by ensuring that day to-day operations are consistently delivered at high standards, with minimal disruption and maximum responsiveness.

KPI	Target	Measurement Method	Reporting Frequency
1.Crime Prevention & Crowd Disruption	≥ 90% of identified threats mitigated before escalation.	Number of criminal incidents and crowd disruptions prevented or neutralized.	• As and when required
2. Response Time to Incidents	Within 24 hours for priority incidents.	Average time taken to respond to threats, or emergencies.	• As and when required
3.Patrol Effectiveness	Minimum of 6 randomized patrols per 12-hour shift.	Number of unpredictable foot and vehicle patrols conducted per shift.	• As and when required
4.Armed Escort Success Rate	100% safe escort completion rate.	Percentage of critical deliveries completed without incident.	• As and when required
5. Asset Protection	≥ 95% interception rate.	Number of unauthorized asset removal attempts intercepted.	• As and when required
6. Body Cam Utilization	100% compliance.	Percentage of tactical officers using body cams during operations.	• As and when required
7.Evidence Management	100% adherence to protocol.	Number of crime scenes managed with proper evidence preservation until SAPS arrival.	• As and when required
8. Operational Reporting	Reports submitted within 2 hours post-incident with ≥ 95% completeness.	Timeliness and completeness of incident and situational reports.	• As and when required

9. K9 Deployment Efficiency	≥ 90% effectiveness in K9 operations.	Number of successful K9-assisted threat detections or deterrence actions.	• As and when required
10. Security Breach Reduction	≥ 30% reduction quarter-on-quarter.	Reduction in security breaches across substations and infrastructure.	• As and when required
11. Screening & Search Accuracy	≥ 98% detection accuracy.	Number of successful detections during screening of people, vehicles, and objects.	• As and when required
12. TRT Readiness & Agility	100% compliance.	• Percentage of TRT members passing monthly readiness and agility assessments.	• As and when required

3.30 Tier-Specific Defence System

To ensure precision in resource allocation, threat mitigation, and performance measurement, NTCSA will implement a Tier-Specific Defence System aligned with Eskom's Enhanced Response Architecture. This framework categorizes all sites into four distinct security tiers based on asset criticality, threat profile, and operational risk.

3.31 Tier Classification and Response Architecture

Tier	Site Type	Threat Profile	Response Architecture	Required Outcomes
Tier 1	National Key Points / High-Risk Infrastructure	Organized crime, coordinated attacks, insider threats	0–30 sec automated detection, ≤3 min tactical response, ≤8 min backup deployment	99% detection, 95% neutralization, zero asset loss

Tier 2	Critical Operational Sites	Copper theft, vandalism, opportunistic crime	0–60 sec detection, ≤8 min mobile patrol, ≤20 min armed backup	97% detection, 90% asset recovery
Tier 3	Standard Operational Sites	Opportunistic theft, trespassing	0–2 min alarm activation, ≤15 min armed response	95% detection, basic protection
Tier 4	Remote Low-Risk Sites	Trespassing, environmental hazards	0–5 min remote alert, 5–30 min response	90% detection, automated escalation

Each tier is supported by a tailored baseline technology stack, including AI-powered CCTV, multi-sensor perimeter detection, biometric access control, and remote monitoring systems. These technologies are calibrated to deliver optimal performance per tier, ensuring cost-efficiency without compromising security outcomes. The service provider is allowed to go beyond the baseline if they feel it will ensure meeting and exceeding expected KPI's.

3.32 Tier-Aligned KPI Calibration

The existing KPI framework will be tier-adjusted to reflect differentiated expectations:

- **Detection Accuracy:**
  - Tier 1: ≥ 99%
  - Tier 2: ≥ 97%
  - Tier 3: ≥ 95%
  - Tier 4: ≥ 90%
- **Response Time Targets:**
  - Tier 1: ≤ 3 min armed response
  - Tier 2: ≤ 8 min patrol, ≤ 20 min backup
  - Tier 3: ≤ 15 min investigation
  - Tier 4: ≤ 30 min remote escalation
- **Threat Neutralisation:**
  - Tier 1: ≥ 98%
  - Tier 2: ≥ 95%
  - Tier 3 & 4: ≥ 90%

- **System Availability:**
  - All tiers: ≥ 99.5%

3.33 Escalation and Accountability

Failure to meet tier-specific KPIs will trigger NTCSA Eskom's Consequence Management Framework, with penalties scaled according to site criticality. Tier 1 breaches will invoke immediate escalation protocols, including forensic investigation, retraining, and potential contract termination.

3.34 Site evaluations

Site visits will be conducted for the successful bidders to verify that they have a functional Control room, legal firearms, Company owned vehicles as well as technologies that were proposed by the bidder.

3.35 Acceptance

This document has been seen and accepted by:
Note: Initials not acceptable

Full Name and Surname	Designation
Melvin Murugen	Middle Manager Security Operations
Baleni Ngwenya	Security Manager
Thomas Tshikalange	Snr Manager Special Project Grids
Dr Remone Govender	Senior Manager Security Solutions

3.36 Revisions

Date	Rev.	Compiler	Remarks
August 2025	0	Christopher Nkosi	First issue

Development Team

3.37

The following people were involved in the development of this document:

Full Name and Surname	Designation
Malusi Jacobs	Senior Advisor Investigation
Melvin Murugen	Middle Manager Security Operations
Jaysen Naidoo	Senior Advisor Investigation
Christopher Nkosi	Senior Advisor Security Operations
Rishigen Naidoo	Senior Advisor Business Intelligence
Siphelele Dlamini	Assistant Officer Security

3.38 Acknowledgements (if applicable)

None

1. TECHNICAL EVALUATION CRITERIA

The appointed service provider must score a threshold of 80% on as per below technical evaluation criteria:

PART A. MANDATORY TENDER RETURNABLES			
No	**Mandatory Tender Returnable**		**Yes/No**
1	Registration of company as a security service provider with PSIRA	Certified copy of company PSIRA certificate issued by PSIRA - check: PSIRA registration number, date of issue.	
2	PSIRA Certificates of Director (s) and ID	for company director(s) minimum grade B (include proof of valid SA identity document).	
3	PSIRA letter of good standing	Certified copy of PSIRA letter of good standing for the security company (Manpower list) - Valid at time of tendering	
4	Private Security Provident Fund compliance letter	Valid letter at time of tendering	
5	Public Liability insurance R 15 million	Valid Letter from insurance company that supplier is in good standing not older than 90 days. -Valid letter from insurance company stipulating that they would have immediate cover from start of contract award. Not older than 60 days.	
6	Valid letter from SAPS	Valid Letter from SAPS issued by the NKP office indicating company's valid registration to offer services at National Key Point. (for services requiring NKP)	
The supplier must have yes for all mandatory requirements to move on to Firearm mandatory (note all certified copies must be less than 90 days unless otherwise specified)			

Part B - FIREARMS MANDATORY			
No	**The Supplier must satisfy ALL Firearm Control Act requirements to be considered for services were firearms are required.**		**Yes/No**
1	Company accreditation with Central Firearm Registry (CFR) by juristic person.	Letter from CFR and verify against Firearm register. - Valid and in company name - SAPS confirmation letter on license firearms available for the company not older than 90 days.	
2	Appointment of the responsible person (Armoury manager) if not the Juristic person /company owner.	(Note: if owner, the responsibility is recorded on CFR letter)	

3	Valid SAPS Firearm competency certificates for responsible person – all accredited firearms in use. (If not owner the appointed person)	Firearm competency certificates (certified copy not older than 90 days)	
4	Valid Training records for responsible person handle and use of firearms for business purposes – all accredited firearms and Knowledge of firearm Control Act (Reg. 21) from a SASSETA accredited institution.	Training records- (Certified copy not older than 90 days)	
5	Annual competency assessment records for responsible person (Armoury manager). (Reg. 21)	Reg 21 records (Certified copy not older than 90 days)	
6	SABS approved safe or strong-room for safekeeping of firearms and ammunitions.	SAPS letter or SABS certificate.	
	The supplier is required to have yes to all the above firearm mandatory requirements to be able to be evaluated on desktop tender returnable and on site.		

Part C - DESKTOP EVALUATION CRITERIA – TENDER RETURNABLE

INFRASTRUCTURE CRIME INVESTIGATION	Weight	Threshold
	100%	**80%**
1.CAPACITY	**45**	
Investigation & Post investigations Support Services (Disciplinary & Criminal) Approach, methodology and tools as outlined in the scope of work Describing in detail the project plan and how this will assist SI in achieving its objectives. Have the necessary technological infrastructure to aid investigation Dedicated teams of fourteen (14) intelligence tactical officers , four (4) forensic investigators, one (1) data analyst , one (1) senior legal Practitioner , experienced in organised crime investigations, armed reaction and intelligence. Demonstrable access to legal team (in-house or outsourced) to assist with prosecutions at own costs.Provide a listing of the staff complement. Each forensic investigation team has 10 years' minimum collective related investigative and intelligence experience	15	
Analytical Capability & Methodology Crime Mapping & Trend Analysis: Use of GIS tools and statistical models to identify hotspots and patterns Predictive Analytics: Ability to forecast criminal activity using historical data and behavioural indicators Data Sources & Integration: Access to diverse datasets (e.g., SAPS, private security, social media, CCTV)Tools & Software: Use of platforms like IBM i2 Analyst's Notebook, ArcGIS, or custom-built dashboards.	10	
Evidence Register Required security infrastructure to safeguard Eskom NTCSA information, data and evidentiary material: • Evidence Safe • Storage for Exhibits	5	

Proper access control to data centres and building		
Polygraph Services Provide the methodology to conduct polygraph test and display the success rate. This must include instrumentation and operations, legal issues concerning polygraph, preparation of testimony, pre and post subject interviews etc. Service Provider qualifications and accreditations to conduct tests (Provide proof of professional body affiliation – American International Institute of Polygraph and or local chapter Being able to compile a detailed report to support the findings Proven ability to testify as an expert regarding the polygraph examination findings Proof of successful execution on previous assignments(references form completed by referee company (not Eskom)	5	
The supplier must provide purchase orders for two previous installations of physical integrated security technology incorporating AI. These installations must demonstrate integration of the following systems: • Alarm system • CCTV system • IACS (Integrated Access Control System) • PA system (Public Address system) • Pre-detection system	10	
2. CONTROL ROOM (Physical Inspection to verify)	**25**	
The control room must be SAIDSA Accredited	2	
Guaranteed communication with all sites (landlines, cellular phones, 2way radios)	2	

Reinforced Doors and walls	2	
Use of online occurrence books	2	
Emergency Call Out Procedure Available	2	
Contingency Plan availability	2	
24 Hour availability	5	
Number of control operators around the clock (minimum 3 operators)	2	
Geographical Information System (GIS) capability in place (Show example)	2	
All employees working with Eskom NTCSA info/data to submit security clearance issued by the SAPS	2	
Original or certified copies of firearm licenses minimum =10 (Pistol & Shotgun)	2	
3. REFERENCES	**15**	
The supplier should provide evidence of at least 3 successful organised crime investigations and successful prosecutions which occurred within the past 5 years.	5	
Proof of current (active) organised crime references not older than 18 Months.	5	
The team should have a collective minimum of 10 years related experience. Provide condensed CV's of each team member.	5	
4. EQUIPMENT AND TECHNOLOGY (Site visits to confirm)	**15**	
Transport – the supplier should have at least 10 vehicles with off-road capabilities, per team (proof must be provided). A list of vehicles must be produced,Certified copies of vehicle registrationcertificates for company vehicles,Proof of any changes in ownership, Proof of valid lease and rental agreements in the name of the Company where	10	

applicable, physical inspection of the vehicles (branding and Km), live monitoring of vehicles, tracking reports. Does the supplier have adequate number of vehicles for the required service , soft and Armoured or reinforced vehicles with: • Two-way radios • Dash cams Are all vehicles fitted with a vehicle tracking system? Are vehicles monitored 24 hours a day, 7 days a week? Does the vehicle tracking system have the capability to produce detailed reports? Are operational vehicles Branded on both sites? Maintenance records for all vehicles? Proof of roadworthiness (Valid License disk)		
Thermal Detection Night Vision Equipment (1 set per team)	2.5	
Air Support manned (drones) with thermal image capability (high capability Pan, Tilt, Zoom)	2.5	
TOTAL	**100**	

The threshold shall be **80%.**

Compiled by:

Name: Christopher Nkosi
Title: Senior Advisor Security Operation
Date: 16/10/2025

Approved/Not approved

Name: Melvin Murugen
Title: Middle Manager Security Operations
Date: 18/10/2025