SCOPE OF THE CONTRACTOR'S SERVICES

SECTION TWO - BACKGROUND OVERVIEW AND SCOPE OF REQUIREMENTS

1. BACKGROUND

Transnet Pipelines, wholly owned by Transnet SOC Ltd is the custodian of the country's strategic pipeline assets. Major operator of 2900km network of crude, gas, and multi-product pipelines in the South Africa economy. The pipeline business handles an annual average throughput of some 16 billion litres of liquid fuel and more than 450 million cubic meters of gases. The liquid products include crude oil as well as diesel, leaded, unleaded, petrol and aviation turbine fuels.

Have over 50 years' experience in pipeline operations (established in 1965) and a strategic player in hydrocarbon transportation in South Africa. Except for the NOC and Island View all depots and Jameson Park accumulation facilities are declared NKP sites. The actual pipeline itself is not a National Key Point.

The liquid fuels network traverses the provinces of KwaZulu-Natal, Free State, Gauteng, Northwest, and Mpumalanga. The intake stations are the two Durban refineries - the crude refinery at Colebrook (Natref) and the Sasol 2 and Sasol 3 synfuel plants at Secunda. The network includes a tank farm, at Tarlton, with a capacity of 30 million litres which is used mainly for storage and the distribution of liquid fuels into Botswana. The gas pipeline, a converted line previously used for liquids, runs from Secunda to Durban via Empangeni. It has take-off points at Newcastle and Richards Bay as well as along the route between Empangeni and Durban.

Pressure in the pipeline network is monitored on a 24 hour-a-day, 365 days-a-year basis at the control centre at Transnet pipelines' Durban head office. The National Operating Centre functions as a planning, control, and security hub. The NOC features state-of-the-art electronic video walls, which monitor and display SCADA (Supervisory Control and Data Acquisition) information, security access control and CCTV feeds from around the network and general information related to the entire pipeline process. The size and complexity of the video system is one of the largest and unique installations in Africa.

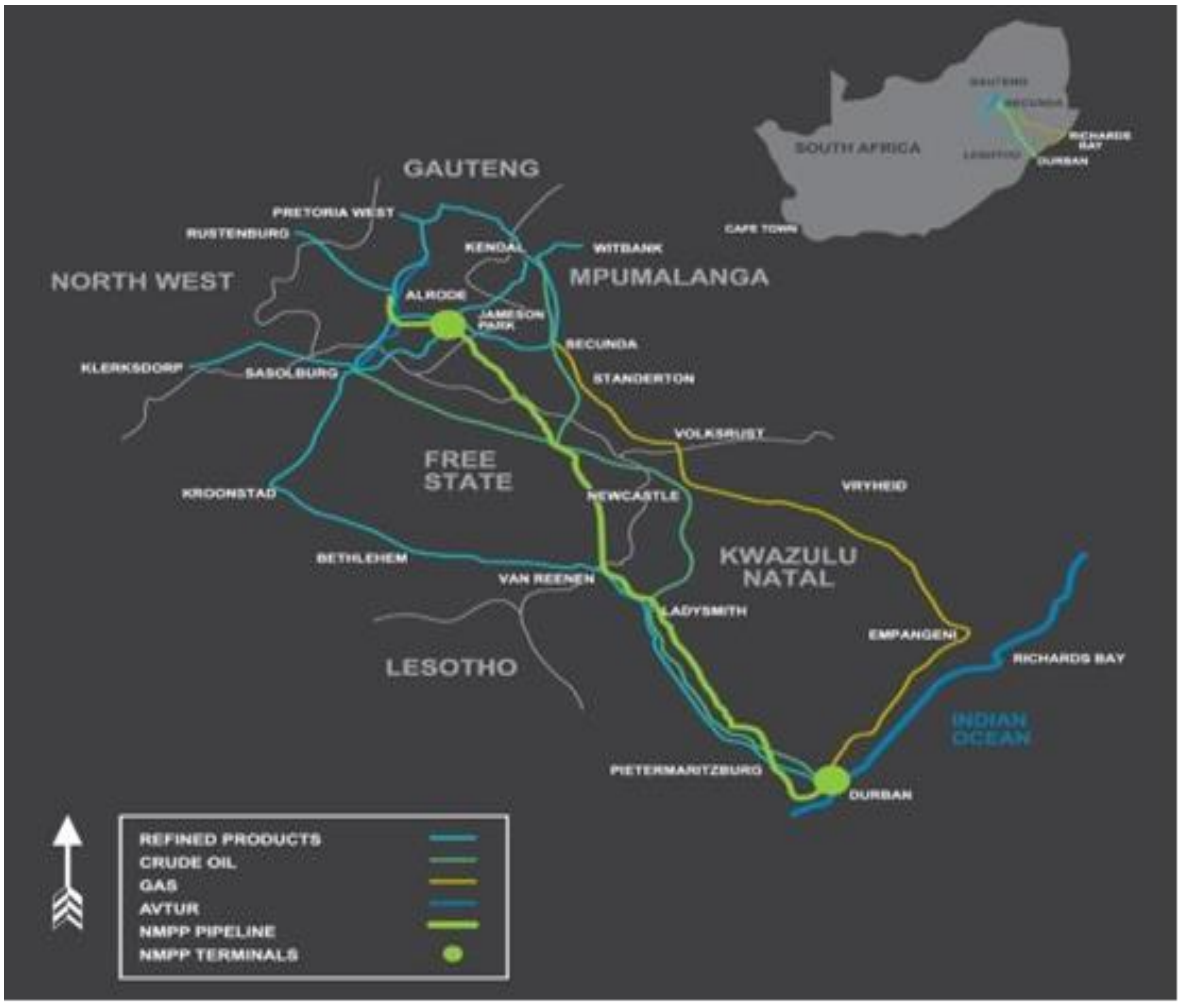
Transnet Pipelines' staff complement of some 600 is deployed across the pipeline network with the business itself being geographically decentralized.

The company owns and operates a 30-million-liter tank farm with road and rail loading facilities in Tarlton to facilitate cross border deliveries via road and rail to Botswana. The company also owns and operates a fractionator plant at Tarlton for the management of intermixture generated.

The company transports approximately 17 billion litres of product per annum and the product slate includes:

- Crude Oil
- Diesel 50ppm and 10ppm
- Unleaded Petrol – 93 Octane
- Unleaded Petrol – 95 Octane
- Jet Fuel
- Gas 600 cubes

The infrastructure to be protected covers thousands of kilometres within the TPL network. The Security department has a hybrid of in house and contracted security personnel. The in-house numbers are very limited and as such Transnet is seeking to partner to provide solutions for its specialized security.



Source: https://www.transnetpipelines.net/wp-content/uploads/2017/05/Operations-Map-Enlarge.png

2. OVERVIEW

Transnet Pipelines requires dedicated RPAS (Drone) services to ensure reliable and uninterrupted services for pipeline operations. The risk to Transnet Pipelines in the event of wilful damage, and the potential capacity loss of the pipeline network and equipment, is too serious to be left to chance. This requirement for effective and efficient security is enhanced by the requirements of the National Key Points (NKP) Act and other relevant security standards and guidelines promulgated by the Government Security Regulator.

The newly enacted Critical Infrastructure Protection Act 08 of 2019 has been gazetted and will repeal the NKP Act after the regulations have been promulgated. The selected service providers must share in the mission and business objectives of the Transnet.

These mutual goals will be met by contractual requirements and new challenges in an environment of teamwork, joint participation, flexibility, innovation, and open communications. In this spirit of partnership Transnet and its service provider/s will study the current ways that they do business to enhance current practices and support processes and systems. Such partnership will allow Transnet to maximise benefits and minimise risk.

Specifically, Transnet seeks to benefit from this partnership in the following ways:

2.1 Transnet must receive reduced cost of acquisition and improved service benefits resulting from the Service Provider's economies of scale and streamlined service processes.

2.2 Transnet must achieve appropriate availability that meets user needs while reducing cost for both Transnet and the chosen Service Provider(s).

2.3 Transnet must receive proactive improvements from the Service Provider with respect to provision of Service and related processes.

2.4 Transnet's overall competitive advantage must be strengthened by the chosen Service Provider's leading-edge technology and service delivery systems.

2.5 Transnet end users must be able to reply on the chosen Service Provider's personnel for service enquiries, recommendations, and substitution.

2.6 Transnet must reduce cost by streamlining its acquisition of Service, including managed service processes on the group basis.

3. SCOPE OF REQUIREMENTS

3.1 Service Description

For reasons stated Transnet Pipelines requires specialized security services in the form of:

a. Specialised Aerial Security Services

The overarching objective of this service is to secure the pipeline, not only from the direct criminals that carry out the activity but also from those criminals that support, organise, and orchestrate crime against the pipeline by creating an integrated, multi-faceted pipeline security service.

- Establish a multi-layered Pipeline security service that leverages appropriate human capital, technology, equipment, and operational procedures to deliver an effective integrated specialised security service.
- Establish a Pipeline Security Protection Services with adequate capacity and capability to deter, detect, prevent, and protect TPL's critical pipeline infrastructure.
- Protect TPL's critical Pipeline infrastructure to contribute towards business continuity, enable product security supply, enable market demand fulfilment, and minimise impact of organised crime.
- Increase the rate of detection, protection, successful apprehension and enable successful conviction.
- Enhance the implementation of investigative & information driven operations to support risk mitigation and critical asset protection.
- Disrupt, dislodge & displace organised crime activities posed against TPL's critical infrastructure deemed as a state asset.

To achieve the above integrated objectives, TPL has structured a specialised integrated security service that includes other disciplines outside of the Aerial Surveillance Services. Due to the criticality of the service, as well as the risk to the critical infrastructure, the service provider will provide a minimum of 8 drones upon award and will be afforded a reasonable mobilisation period of up to three (3) months to meet the deployment requirements in respect of all RPAS (Drone) deployment requirements (e.g., equipment, registration, personnel, supporting infrastructure, etc), should it be required.

3.2 Scope of works

3.2.1 General

- Provide a mission-ready capability in line with TPL requirements
- Effectively apply the Intelligence Life-cycle Model to execute intelligence driven operations.
- Effectively plan and conduct specialised security operations.
- Effectively prepare and exercise operational capability for operational readiness, preparedness & execution.
- Assess situations, make critical decisions, and direct actions enabling risk mitigation & ensuring critical asset protection as per Minimum Physical Security Standards (MPSS).
- Conduct required liaison, joint planning and execution with relevant stakeholders participating in integrated security solution.
- Plan, arrange and coordinate effective and efficient support for internal & external specialized security operations.
- Coordinate movement of own capabilities when executing operations.
- Plan and conduct tactical aerial and information driven actions.
- Provide input, test, improve and recommend continuous improvement for the integrated security best practice methodology.
- Provide input, develop, and manage own situational awareness.
- Collect, collate, analyse, generate, and disseminate information for the successful execution of integrated specialised security operations.
- Plan and effectively implement operational security (OpSec) as per Minimum Information Security Standards (MISS).
- Develop, maintain, and review operational, risk-mitigation and contingency plans.
- Develop, implement, and review appropriate standing-operating-procedures that encapsulates the integrated specialized security service as well as improvements from operational research from time to time.
- Provide qualified/serviceable: Personnel; manned and unmanned (RPAS) vehicles; field equipment; infrastructure; weapons; communications and technology as specified in support of specialized security operations.
- When required, availing the selected personnel for Voice Stress Analysis & Polygraph assessments.
- Conduct operational research on specified capability areas and disciplines; and
- Provide the necessary regulatory requirements monitoring, enforcement & reporting for all specialized security operations to ensure compliance and ensure professional conduct of the highest order.

3.2.2. RPAS (Drone) Services

The service provider will be required to carry out the following activities:

- Conduct effects-based operations in conjunctions with other disciplines (i.e., Law enforcement, Specialized Operations, Helicopters, Investigations, Business Intelligence, Information Management & Advocate).
- Detect suspicious vehicles, persons, and evidence of suspicious activity on or nearby the pipeline servitude.
- Direct Mobile Response Security Teams (MRST) to crime sites as well as to direct them to criminals hiding under cover of darkness and in vegetation.
- Provide a 24-hour operational service (day and night operations).
- Report on any and all anomalies found on the network and in proximity to the network.

- Have effective communication with its own Security Control Room, MCC and other security teams and disciplines.
- Demonstrate capacity of pilots and support staff (at least 16 teams) that can operate systems in the form of experience and licensing. The bidders must supply, as a returnable document, a detailed list of all pilots that is going to be utilized for the contract, specifying the respective role/s they will fulfil.
- Provide RPAS surveillance as a service, where they own the RPAS infrastructure, they operate the RPAS, do the maintenance of the RPASs and they are liable for any damage that the RPAS may cause due to RPAS issues (e.g., loss of control and loss of power of RPAS that may lead to crashes).
- This process will be supported by suitable AI technology means with the capability and capacity to automatically process any form of information input to generate security advisory, operational guidance and reporting to Business Intelligence as well as all other disciplines
- Have the capacity for the operation of the RPAS surveillance teams to the specific provinces as they will be a need to rapidly deploy and change location of the RPAS service. Location of deployed teams will change due to incidents and change of high-risk areas, operational requirements, Crime trending and patterns.
- Have the capacity that includes pilots that can operate RPAS, and these pilots must have the necessary experience and licensing. The entire crew for the RPAS operational teams must be proven (all licensing for crew).
- Own and/or be in a position to supply the entire RPAS infrastructure and execute specialised security operations immediately upon appointment.
- Take responsibility for any damage that the RPAS system may cause or impart on any other infrastructure.
- Take responsibility for any penalties due to infringement on the operational capacities.
- Have capacity or prove that they can source the capacity for the operation of the RPAS surveillance teams for immediate operational execution, for duration of 3 (three) years and must have the capacity to relocate team as per TPL request within the five mentioned provinces.
- Except where otherwise stated in this specification, all equipment, installation must conform to the latest recommendations of the ITU-T, SANS, ISO, IEEE, SABS, CENELEC and IEC standards.
- All standards and requirements in this document must be adhered to and any deviations must first be discussed with the Security department. Such proposed deviations can only be deemed accepted by TPL when confirmed in writing and duly signed by the Delegated Authority.
- Operate in an environment where there are no runways so all RPAS used to provide this service will not require a road as a pre-requisite for take-off and landing.
- Provide for continuous surveillance video material and upload during flight time will be required.
- Be responsible for any harm or damages that their equipment causes during and after operation; and

- All video footage must be time and GPS stamped & authenticated. It must also be available for viewing and download through secure authentication on the webpage application.

RPAS Operational Requirements:

- Day and night operations in varied weather conditions
- Beyond-Visual Line of Sight (B-VLOS) Operations of a minimum of 10kms from the Remote Pilot Station in either direction.
- Batteries should last for a minimum of one hour (60 minutes) of continuous use before a change is required.
- Battery changes should be completed on a "Hot Swap" basis.
- RPAS should be licensed to:
    - Operations overhead of any person or group of people or within a lateral distance of 50m.
    - Operations within a lateral distance of 50m from any structure or building
    - Operations over a public road, along the length of a public road or at a lateral distance of less than 50m from a public road.
    - Operations adjacent to or above a nuclear power plant, prison, police station, crime scene, court of law, national key point, or strategic installation
- Use of any public domain or private property where permission is granted as a place of take-off or landing of an RPAS; and
- Remotely piloted aircraft to be used to conduct surveillance of the pipelines on a 24-hour basis, 7 days a week.

RPAS Technical Requirements

- High-Definition recorded surveillance video material for the length of the shift.
- Capacity to relay/store live footage video on secure server
- Camera resolution 1080p or more with x 9 optical zoom capability. Variable resolution (1080p, 720p, 480p to UHD) for surveillance and central location transmission (real time reporting).
- Ability to provide visual footage in the event of visual impairments (e.g. Smoke, Fog, Mist, etc)
- Stability control functionality in order to ensure clear footage is captured to support prosecutions, investigations and tracking
- Day/night minimum 4K camera, thermal and optical camera functionality – minimum 8MP (mega pixel) resolution.
- GPS enabled – drone to have a real time tracking and monitoring capabilities. Flight path following.
- Drone must have a "follow me" function.
- Drone moving speed of a minimum of 5m per second, which is 18km/h per hour.
- Drone capacity to fly "Beyond Visual Line of Sight – Civil Aviation Authority BVLOS approval.

3.3 Operational Environment

3.3.1. The Operational Area of Responsibility of Transnet Pipelines encapsulates the

National deployment of the Pipelines Network, which includes the Head Office in Durban, its National Operations Centre (NOC)/ MCC in Pinetown and all its depots, block valves and pipelines.

3.3.2. The area and network incorporate the following key routes:

- Jameson Park to Watloo via Alrode
- Jameson Park to Rustenburg via Alrode
- Durban Island View Pumpstation to Langlaagte
- Watloo to Kendal
- Witbank to Secunda via Kendal
- Secunda to Jameson Park (via Sasolburg)
- Colebrook to Klerksdorp via Sasolburg
- Colebrook to Kroonstad via Sasolburg

3.4.3 Although the pipeline traverses and overlaps into the other areas, the operational terrain of Transnet Pipelines is divided into three separate areas, namely:

Sector Alpha - Encapsulates the network from:

- Kroonstad to Sasolburg (110 km)
- Sasolburg to Colebrook (10km)
- Sasolburg to Klerksdorp (138km)
- Alrode to Rustenburg (127 km)
- Alrode to Watloo (87 km)
- Eldorado Park to Pretoria West (18 km) **Total 490 kilometres**

Sector Bravo - Encapsulates the network from:

- Jameson Park to Kendal (81 km)
- Jameson Park to Colebrook (70 km)
- Jameson Park to Alrode1 (46 km)
- Jameson Park to Alrode2 (42 km)
- Kendal to Secunda 12 inch & 20-inch same servitude (72 km)
- Secunda to Jameson Park (75 km)
- Witbank to Kendal (30 km)
- Kendal to Watloo (90 km) **Total 506 kilometres**

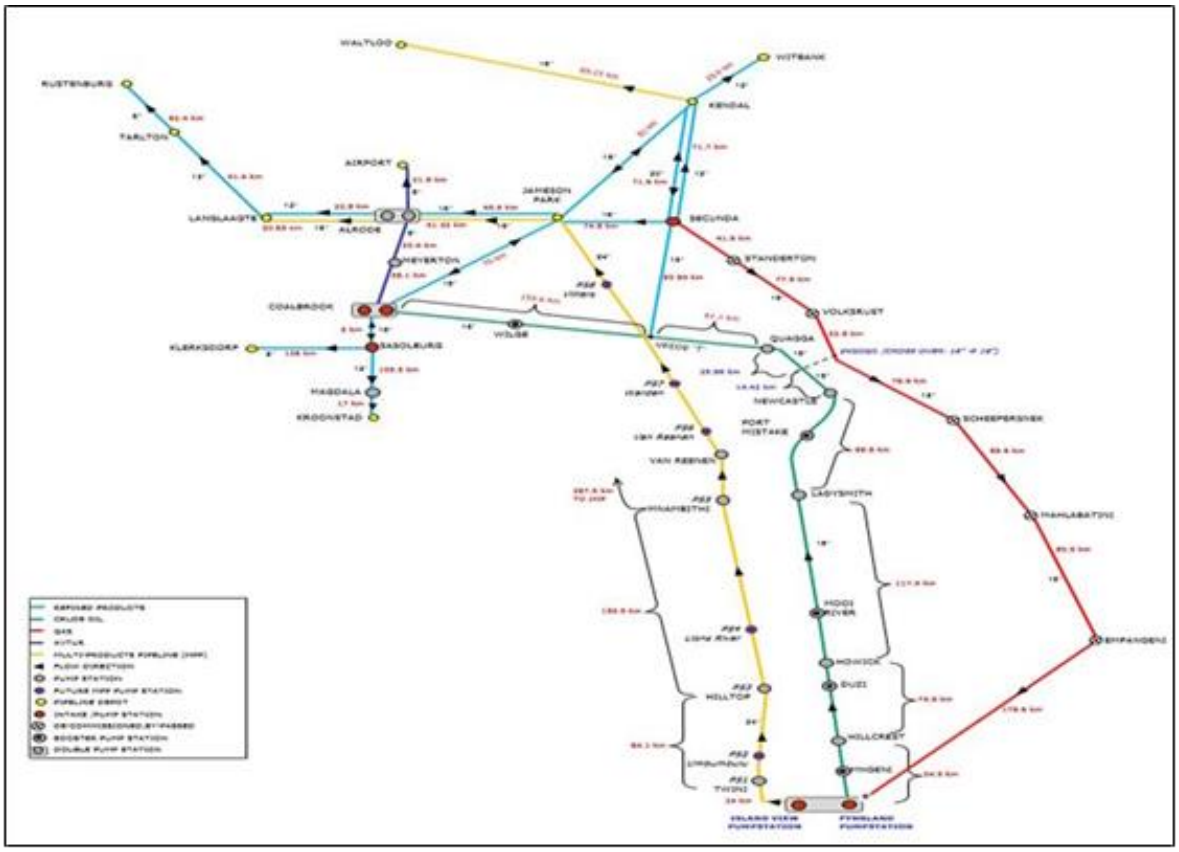
Sector Charlie - Encapsulates the network from:

- Jameson Park to Villiers (75 km)
- Villiers to Warden Station (105 km)
- Warden to Mnambathi Station (157 km)
- Mnambathi Station to Hilltop (150 km)
- Hilltop to Twini Station (85 km)
- Twini to Island View (24 km) **Total 596 kilometres**

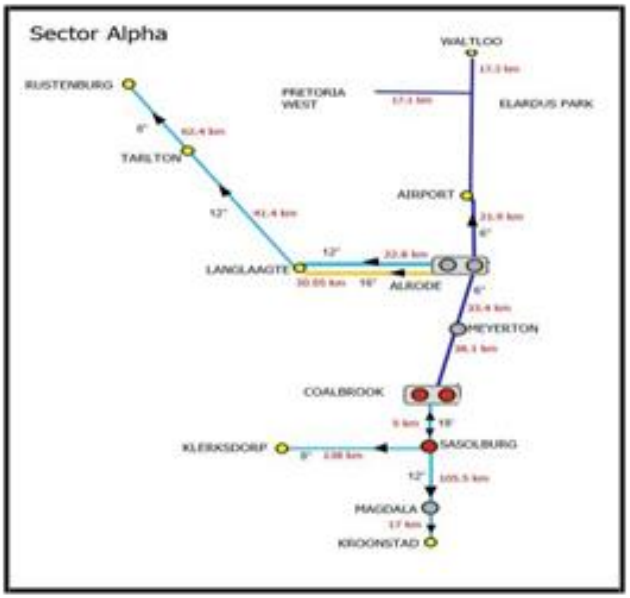
Block valve Positions

There are approximately 250 block valves within the three sectors that need protection from criminals. The block valves are key components of the infrastructure, and the exact location cannot be shared on this tender due to the sensitivity thereof. The successful bidder will be provided the details and locations of these block valves. The exact details and photographic depictions will be made available during the tender briefings and site inspections.

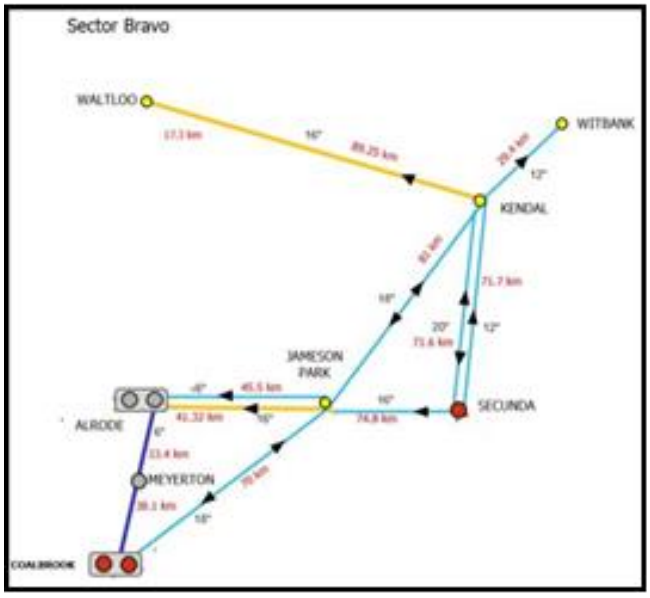
Total 1608 kilometres
Active pipeline 2518km's
In-active pipeline 565km's
Totalling: 3083km's
Transnet Pipelines Overall (Geographical Positioning)



Sector Alpha (Geographical Positioning)



Sector Bravo (Geographical Positioning)



Sector Charlie (Geographical Positioning)