SCHEDULE 1 – SCHEDULE OF REQUIREMENTS

DESCRIPTION	**STANDARD TERMS AND CONDITIONS FOR THE PROVISION OF RAIL NETWORK PROTECTION SERVICES (RNPS) TO TRANSNET RAIL INFRASTRUCTURE MANAGER (TRIM) WITHIN THE CENTRAL CORRIDOR FOR A PERIOD OF TWELVE (12) MONTHS.**
SERVICE PROVIDER	**……**
CONTRACT NUMBER	**TRIM/2026/06/1447/7536/RFP**
DURATION	**TWELVE (12) MONTHS**
COMMENCEMENT DATE	**……**
EXPIRY DATE	**……**

With reference to the Standard Terms and Conditions of Contract, Reference Number TRIM/2026/06/1447/7536/RFP dated …… , ("Contract") between Transnet SOC Ltd ("Transnet") and …… (the "Service Provider") pursuant to which you have agreed to perform certain services for and on behalf of Transnet subject to such Contract.

The defined terms in the Contract will, unless otherwise indicated, have the same meaning in this Schedule of Requirements. In consideration of the mutual covenant and agreements contained in the Contract and in this Schedule of Requirements, it is agreed as follows:

1. Description of the Services

The scope of Services to be provided by the Service Provider is the Provision of Rail Network Protection Services (RNPS) to Transnet SOC under the Operating Division of the Transnet Rail Infrastructure Manager (TRIM) within the Central Corridor for a period of Twelve (12) months. The details for the Services to be provided are as stipulated in clause 2 below.

2. Scope of Services

1.1 Scope of works

The requirements outlined in the scope of work are to ensure that the SSPs achieve the Security Management Life Cycle (SMLC) as outlined below to secure the personnel, infrastructure, and assets adequately. The elements of the SMLC help to establish a mindset for protecting assets.

1.2 Deter threat function

To convince the intruder to turn around and not attempt the planned intrusion, resulting in a successful deterrent. This can be achieved by dissuading criminals by turning your assets into undesirable targets through installation of visible signage indicating the presence of security systems, dogs, arrest, intelligence, detection technologies, security officers, etc.

1.3 Deny threat function

The next step following failure to deter threat is to deny them access to your assets. This is achieved by implementing target hardening solutions such as fencing, door locks, tamper proof enclosures for trackside assets, steel, concrete, re-enforced protection for assets, sleepers on top of signalling cable trenches, very heavy lithium batteries, ferrous and non-ferrous metals, etc.

1.4 Detect threat function

To achieve awareness of the intruder and thus allow timeous response to the intrusion. This is achieved by installing high-tech detection methods that shall alert the organisation when there is an unauthorised entry at a secured site/rail line/facility.

1.5 Delay threat function

If the attempts to deter, deny and detect the threats have failed, the next best thing is to delay entry into the secured site. The longer you delay the intruder, the more time the response teams have to arrive. This can be achieved by triggering fight back systems that can be activated from the control room.

1.6 Defend/Detain threat function

Activate the response teams to the intruded site and provide them with all information on the security systems. This shall empower the response teams with a full knowledge of what to expect on site.

1.7 Community engagement

The Service provider shall provide a plan to engage the community stake holders and establish partnerships with them to get the buy-in and mitigate the security challenges in the Central Corridor. The plan shall the following:

- Engage community stakeholders and establish partnerships with them.
- How to support an integrated approach by influencing socio-economic initiatives through the introduction of small businesses into the value chain and innovative upliftment of the community through skills development.
- How to establish full-time sources of information from local communities such as liaison officers within the local communities, to source information about crime/incidents within the rail network, identify syndicates operating within local communities, and incorporate local communities in a performance, success, and reward model to look after the railway infrastructure that runs near the communities.

1.8 Community engagement plan to mitigate crime and incidents. The plan must fully cover the following:

• Minimum 2 community engagements per quarter for the duration of the contract.

• A plan on how to support an integrated approach by influencing socio-economic initiatives through introduction of innovative upliftment of community through security related skills development throughout the Central Corridor.

• The SSP shall submit a minimum of two letters of intent, duly signed and stamped by the SSP, the relevant community leader, and tribal leader. The letters shall confirm the community and tribal leader's commitment to support the SSP as part of community engagement process.

1.9 Law Enforcement Agencies

The Service Provider shall provide a plan to interface with the Law Enforcement Agencies (E.g., Police, Community Forums, security committees, mining crime combating forums, etc.) and industries (E.g., farmers' associations, Ferrous and Non-Ferrous Committees, etc)

to mitigate the security challenges in the Central Corridor. The plan shall include but not be limited to the following:

- Establish a dedicated investigation team that adequately supports the crime stats provided to manage all reported Transnet incidents, case management, establish an information network within their areas of responsibility, follow up on reported cases with the National Prosecuting Authority (NPA) and update Transnet on the status of all cases.
- How to improve existing cooperation, coordination, and strengthen information sharing with Law Enforcement agencies.
- How the Service Provider shall conduct data analysis and a further plan on how to execute joint operations with other relevant stakeholders.

1.10 <u>Physical resources required</u>

RESOURCE DISCRIPTION	**QUANTITY**		**TOTAL RESOURCES**
DAY		NIGHT	
Foot Patrollers Unarmed Grade C (Substation, Relay Room, Depot Yards)	175	182	357
Foot patrollers Unarmed Grade C (Servitude)	209	243	452
Crime Prevention Armed Driver Grade C	76	90	166
Crime Prevention Armed Crew Grade C (1 x Per Vehicle 10 000km pm)	76	90	166
Crime Prevention Vehicle (Double Cab 10 000km pm)	76	90	90
Tactical Team Leader/ Driver Armed Grade B	12	17	29
Tactical Team Armed Crew Grade C (2 x Per Vehicle)	24	34	58
Tactical Vehicle (Double Cab 10 000km pm)	12	17	17
Equestrian (Horse covering maximum 2km)	10	12	22
Armed Horse Rider Grade C	10	12	22
Crime Prevention Motorbikes	11	13	13

Crime Prevention Motorbike Rider Armed Grade C	11	13	24
K9 (for critical facilities: diesel depot, material stores)	3	5	8
K9 Handler Armed Grade C	3	5	8
Drone Team (Includes Drone Operator, Drone Equipment, Vehicle, and Support Protection) (Drone specifications: water resistant thermal camera, 10km radius capability, 8 hour shift per day)	0	5	5
Community engagement	0	0	8
Supervision (Grade B armed)	24	24	48
Supervisor Vehicle (Single Cab 10 000km pm)	24	24	24
Control room supervisor (Grade B)	1	1	2
Control room operator (Grade C)	6	6	12
Area Managers (Grade A)	6	0	6
Investigations team (Grade A)	3	0	3
11 x Days Shutdown (First shut January 2027)			
Grade "C" - Unarmed Dayshift (Foot patrollers)	56	56	112
Crime Prevention Armed Driver Grade C	10	10	20
Crime Prevention Armed Crew Grade C (1 x Per Vehicle 10 000km pm)	10	10	20
Crime Prevention Vehicle (Double Cab 2 000km pm)	5	0	5
Drone Team (Includes Drone Operator, Drone Equipment, Vehicle, and Support Protection) (Drone specifications:	2	0	2

water resistant thermal camera, 10km radius capability, 8 hour shift per day)			
11 x Days Shutdown (Second shut)to be confirmed)			
Grade "C" - Unarmed Dayshift (Foot patrollers)	56	56	112
Crime Prevention Armed Driver Grade C	10	10	20
Crime Prevention Armed Crew Grade C (1 x Per Vehicle 10 000km pm)	10	10	20
Crime Prevention Vehicle (Double Cab 2 000km pm)	5	0	5
Drone Team (Includes Drone Operator, Drone Equipment, Vehicle, and Support Protection) (Drone specifications: water resistant thermal camera, 10km radius capability, 8 hour shift per day)	2	0	2

1.11 Background

The Central Corridor is a strategic and important go-through passage for different corridors. Transnet's primary business is to provide rail transport of commodities for the export, regional and domestic markets. Transnet operates the world-class heavy-haul coal and iron ore export lines and is developing the manganese export corridor to heavy-haul standards.

Transnet also transports a broad range of bulk general freight commodities and containerised freight. The division maintains a complex rail network of approximately 31 000 track kilometres (20 900 route kilometres) over which commodities are railed.

The diverse rail network comprises 1 500 kilometres of heavy haul lines and includes 3 928 kilometres of branch lines that serve as feeders to main lines. The rail network service provides strategic links between ports, terminals and production hubs, providing connectivity within Southern African railways to support regional integration. Infrastructure connectivity, coupled with close co-operation with other Operating Divisions and collaboration with key customers, enables the delivery of freight volumes across value chains.

Transnet introduced a new operating model that shall decentralise key responsibilities to ensure a more responsive rail freight network that is better equipped to service the South African economy. The Central Corridor specifically is divided into sectors below:

Cluster 1 (Sentrarand and lines, Leeuhof, Sasolburg, Potchefstroom, Klerksdorp and Lines)

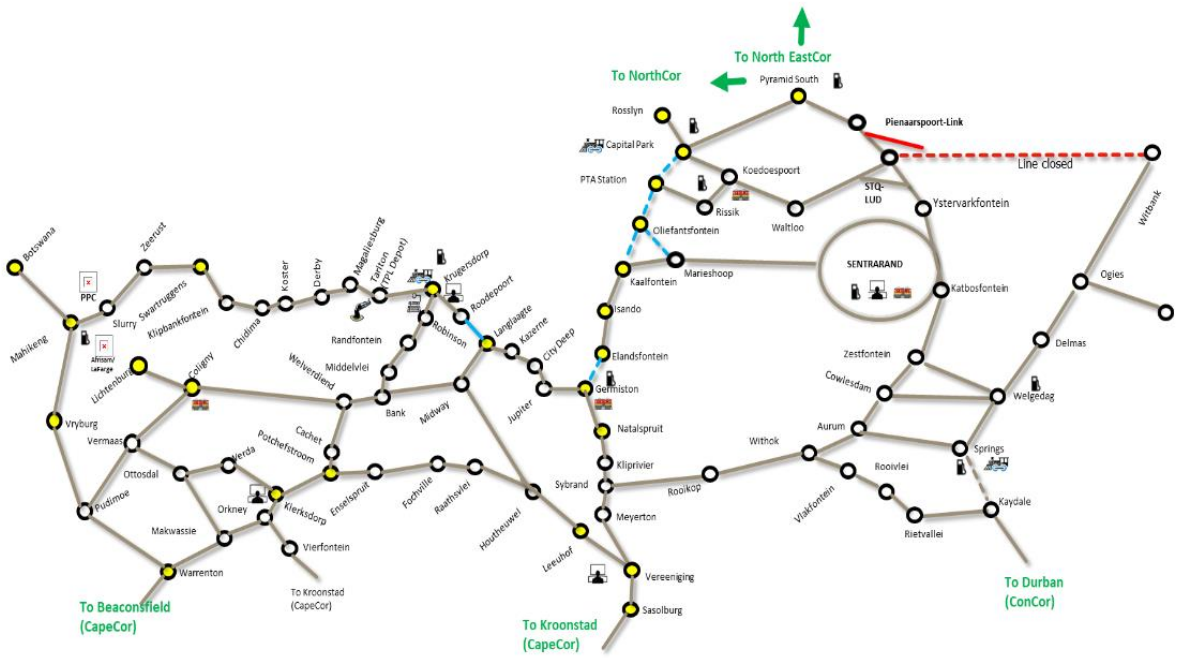
Cluster 2 (Elandsfontein, Marieshoop, Springdale, Kaalfontein, Pretcon, Capital Park, Watloo & Greenview and lines, Natal Spruit yard and lines.)

Cluster 3 (Klerksdorp and lines, Mafikeng and lines.)

The Central Corridor has critical infrastructure below.

- Length of the rail network – 2818 Kilometers (km)
- Total traction Sub = 58 (24 sites have existing technology)
- Total distribution Sub = 41 (1 site has existing technology))
- Total relay room = 107 (25 sites have existing technology)
- Depots= 3
- Yards= 35 (11 sites have existing technology)

The Central Corridor is illustrated on the map below:



1.12 Current Situation

Cable theft is the most severe of the security threats in the Central Corridor. The rail-related infrastructure, rolling stock and perway below are also marred by relentless theft and vandalism.

Infrastructure (Operational yards, depots, Operational bays, OHTE, underground cable, signalling cable, relay rooms, substations, tie stations, bridges, warehouses, CTC buildings, signal and infra depots, telecommunications high sites, Fibre-optic cables, concrete enclosure, apparatus boxes, track side boxes, points machines, rail-related theft, Motor traction cable, reefer container cable and refrigeration system,

inaccessible service roads due to high vegetation, branch line infrastructure malicious damage, vandalism of condition monitoring technologies, Perway vandalism, wrecks along the railway line from previous incidents, material stockpiles along the railway line, etc.).

Assets [Condition Assessment System (CAS), locomotives, wagons, railway line, rails, pendrol springs and other rail fastenings, locomotive batteries, tarpaulins, containers, signalling, point machines, etc.].

Commodity (Example, Chrome, manganese, sugar, wood, automotive, fuel, diesel, coal, etc.).

There are also other related security issues below which have an adverse impact on rail operations in the Central Corridor.

Security Officer Management and supervision (Collusion, lack of supervision, etc.).

Illegal occupation of the Rail reserve (Highly densified with encroachment, dilapidated buildings along the sections, etc.)

Lack of stakeholder engagement (Access to farms for patrol purposes, Community service disruptions, Animal collisions, railway line running through private properties, Municipal and a vast domination of Tribal Authorities in the Central Corridor, lack of crime intelligence, etc).

2. COMPLIANCE AND STANDARDS

2.1. The Service Provider shall submit the following documents as mandatory returnable documents. Compliance with all applicable legislation shall be at the SSP's cost. The Service Provider shall be liable for any breach by any one or more of its security officers, employees, permitted agents, and contractors (independent or otherwise) of the provisions of these clauses and hereby indemnifies and holds the Client harmless against all claims, loss, or damage which the Client may suffer arising out of all such breaches.

2.1.1. The Service Provider shall provide a valid PSIRA certificate as a security provider in terms of section 20 of the PSIRA Act. ("New Certificate" in line with industry circular issued by PSIRA on 10 March 2015). The SSP shall ensure that it obtains and retains its PSIRA registration certificate. The PSIRA certificate must be valid on the closing date and time of the bid.

2.1.2. The Service Provider shall provide proof of Public Liability Insurance cover from Insurer for Public Liability Insurance (PLI) cover for not less than R5 000 000,00 (Five million South African Rand) with an annual limit cover of not less than R30 000 000,00 (Thirty million South African Rand).

2.1.3. The Service Provider shall provide proof of Security Liability Insurance cover from the Insurer for Security Liability Insurance cover for not less than R5 000 000,00 (Five million

South African Rand) with an annual limit cover of not less than R30 000 000,00 (Thirty million South African Rand).

2.1.4. The Service Provider shall submit a letter of compliance from the Security Industry Provident Fund. The letter of compliance shall not have any outstanding amounts.

2.1.5. The Service Provider shall submit a letter of Good standing from the Security Industry Medical Aid Insurance/Fund. The letter of Good standing shall be accompanied by a Human Resources (HR) list of employees.

2.1.6. The Service Provider shall provide valid proof of PSIRA (Grade A or Grade B) credentials for each active Member (Director, Partner, Trustee) of the bidding company. The PSIRA certificate must be valid on the closing date and time of the bid.

2.1.7. The SSP shall submit a valid Criminal Clearance Certificate(s) from the South African Police Services (SAPS) for all Company active Directors. Third party issued criminal clearance certificates will not be accepted. The extent of the clearance shall be in line with the Schedule Table of Offences of the Private Security Industry Regulation Act, 2001. The criminal clearance certificate(s) shall not be older than six (06) months.

2.1.8. The Service Provider shall submit a valid and signed Letter of good standing from PSIRA. The letter of good standing shall be on PSIRA letterhead.

2.1.9. The Service Provider shall submit a signed Letter of Good Standing from the Compensation fund for Occupational Injuries and Diseases Act (COIDA).

2.1.10. The bidding company's security personnel must be registered with PSIRA. The Service Provider shall submit valid PSIRA registration certificates (Minimum Grade C) of at least Five (5) security officers currently employed by the Service Provider to prove compliance.

2.1.11. The bidding company's security personnel who are required to use firearms shall have SAPS firearm competency certificate. The Service Provider shall submit a minimum of five (5) SAPS firearm competency certificates for five (5) security personnel in their employment. The competency certificate must not be older than 5 years.

2.1.12. The bidder shall submit a list issued by the SAPS Central Firearm Registry, indicating a minimum of two hundred and fifty-seven (257) firearms registered in the name of the bidding company

2.1.13. Bidders must submit a valid copy of the Performing Animal Protection Act License (PAPAA Act) for the province in which the service will be provided. The bidding company shall submit the PAPPA license for Gauteng province. The licenses accepted must be in the name of the bidder or a third-party contracted service provider (Animal and handler services).

2.1.14. Bidders must submit a valid copy of the Performing Animals Protection Act License (PAPAA Act) for the province in which the service will be provided. The Service Provider shall

submit the PAPPA license for Northwest Province. The licenses accepted must be in the name of the bidder or a third-party contracted service provider (Animal and handler services).

2.2. Compliance with statutes

2.2.1. The Service Provider shall comply with all relevant legislation as amended from time to time, including, but not limited to, the ones below. Compliance with all applicable legislation shall be at the Service Provider's cost.

2.2.1.1. PSIRA Act (56 of 2001), as amended;

2.2.1.2. Private Security Industry Levies Act, (23 of 2002);

2.2.1.3. National Key Points Act (102 of 1980), as amended;

2.2.1.4. Basic Conditions of Employment Act (75 of 1997);

2.2.1.5. Compensation for Occupational Injuries and Diseases Act (130 of 1993), as amended;

2.2.1.6. Provincial ordinances and laws and municipality by-laws including all relevant regulations promulgated;

2.2.1.7. The Occupational Health and Safety Act (83 of 1993);

2.2.1.8. Protection of Personal Information Act (4 of 2013);

2.2.1.9. Firearms Control Act, (60 of 2000), as amended;

2.2.1.10. Criminal Procedure Act (51 of 1977);

2.2.1.11. Control of Access to Public Premises and Vehicles Act (53 of 1985), as amended;

2.2.1.12. Codes of Good Practice embodied in the Broad Based Black Economic Empowerment Act (53 of 2003);

2.2.1.13. Independent Communications Authority of South Africa Act (13 of 2000), as amended;

2.2.1.14. Legal Succession to the South African Transport Services Act (9 of 1989);

2.2.1.15. Income Tax Act (52 of 1962);

2.2.1.16. Value-added Tax Act (89 of 1991);

2.2.1.17. Trespass Act (6 of 59)

2.2.1.18. Matters Amendment Act (18 of 2015);

2.2.1.19. Any other legislation and regulations and/or in-house specific policies, procedures guidelines that govern some of the Client's sites; and

2.2.1.20. Any other regulatory obligation such as the Railway Safety Regulator (RSR) Act (16 of 2002).

2.3. Shutdown costs

2.3.1. TRIM schedules two shutdowns of 11 and 14 days each within identified sections of the corridor to carry out maintenance and repairs on the railway infrastructure.

2.3.2. The shutdown periods typically experience heightened criminal activity. Accordingly, specialised security services are required to provide protection during the shutdowns for a period not exceeding 14 days per shutdown.

2.3.3. The bidding company shall provide a quote for 2 annual shutdowns in the Central Corridor over a 12-month period.

2.4 Delivery, Risk and Ownership

The Service Provider must during the Contract period utilize and maintain the Hardware and Software, however Transnet remains the owner.

The Service Provider shall be liable for and shall, at its own cost and expense, provide maintenance services and replace, repair, and make good any damage howsoever to the Hardware and/or Software during the Contract period to ensure that the system is always in good working order and meet the required functionality.

The Service Provider shall carry all the risks of the Hardware and Software during the Contract Period. The Risk of the Hardware and Software shall only pass to Transnet upon Transent becoming the owner of Hardware and Software.

The Service Provider shall ensure that the latest released versions of the Software (if applicable) are supplied and installed in the Systems for the Contract period.

Ownership of hardware and software shall vest in Transnet immediately upon the expiry of the Contract Period. Upon this event, Transnet shall not be liable for any further payments to the Service Provider in terms of this Agreement. For the sake of clarity, no residual amount shall be payable to the Service Provider upon the expiry of the contract period.

3. Contract Manager/s & Personnel to provide the Services

Transnet Contract Manager	
Designation	
Operating Division	
Address	
Telephone	
Email	

Service Provider's Account Manager	
Designation	
Address	
Telephone	
Email	

4. Performance Review Meetings

Contract management and performance review meetings will be held on a monthly basis as required by Transnet's Contract Manager with adherence to the applicable KPI Matrix.

5. Fees & Disbursements

5.1 In consideration of the performance of the Services by the Service Provider pursuant to this Work Order, Transnet will pay to it an amount not exceeding the accepted quotation for the twelve (12) month period.

IN WITNESS of which this Schedule of Requirements has been duly executed by the parties.

SIGNED for and on behalf of

Xxxxxxx

Signature.....

Name.....

Position.....

Date.....

SIGNED for and on behalf of

Transnet SOC Ltd

Signature.....

Name.....

Position.....

Date.....

SIGNED for and on behalf of

Transnet SOC Ltd

Signature.....

Name.....

Position.....

Date.....

APPENDIX 1

Address for Notices

Any notice or communications between the parties to be given under this Agreement shall be deemed to have been received at the following times:

i. by email transmission – when the sender receives confirmation of receipt;

ii. by hand delivery - immediately upon receipt by the recipient.

Any notice or communications between the parties shall be delivered to the addresses set out below:

The Service Provider	**Transnet**
Addressee:	Addressee:
	Transnet SOC Ltd
Attention:	Attention : Group Legal Counsel
Physical Address:	Physical Address:
Postal Address:	23rd Floor Carlton Centre 150 Commissioner Street Johannesburg 2001
	Postal Address:
	P.O. Box 72501
	Parkview
email:	email:
xxxxxxx@cccccccc	xxxxxx@transnet.net

Either party may, by a notice given in accordance with this Schedule 1, change its address or email address for the purpose of this Schedule 1.

APPENDIX 2

Non- Disclosure Agreement

Date: …… 20--

I (*name*) …….

Of (*address*) …….
…….
…….

Undertake to Transnet SOC Ltd ("Transnet") that:

1. I shall keep confidential and not to disclose or make available to any third party, except with the express prior written consent of Transnet, any Confidential Information relating to Transnet business, assets, customers or staff which is disclosed to me or to which I may have access during the course of providing Services to Transnet ("my assignment"); and

2. Upon termination of my assignment, I shall return to Transnet all documents, books, discs, tapes or other records (in whatever medium) which I may have in my possession, custody or control and which are the property of Transnet, its customers, staff or agents and any copies thereof.

For the purposes of this Confidentiality Agreement, "Confidential Information" shall mean any information in whatever form including, without limitation, any information relating to systems, operations, plans, intentions, market opportunities, know-how, trade secrets and business affairs of the Transnet Group or its customers, whether in writing, conveyed orally or by machine-readable medium.

I understand that this Confidentiality Agreement shall survive the termination of my assignment.

SIGNED at _____ on _____20--

(Signature) ……

in the presence of:-

Witness name: …….

Witness Signature: …….

Witness address: …….

…….