

TRANSNET RAIL INFRASTRUCTURE MANAGER (TRIM)



Scope Of Work [SOW]

The purpose of this guidance document is to outline the technical specifications required in the intended tender and receive approval for the specifications from all stakeholders prior to the creation of a business case/tender. This document sets out the key areas that should be included in a specification document.

LEGAL REQUIREMENTS FOR ALL SECURITY CONTRACTS

- *A Baseline Risk Assessment needs to be done for ALL security contracts, regardless of the value of the contract*
- *The Health and Safety specifications need to be based on the outcome of the Baseline Risk Assessment*
- *The cost of Health and Safety needs to be included in the Bill of Quantities. This is to ensure that the principal contractor makes adequate provision for the costs of meeting the minimum legal health and safety requirements.*

PROJECT TITLE: Provision of Rail Network Protection Services (RNPS) to Transnet Rail Infrastructure Manager (TRIM) within the Central Corridor for a period of Twelve (12) months.

Provision of
 Provision of Rail Network Protection Services (RNPS) to Transnet Rail Infrastructure Manager (TRIM) within
 the Central Corridor for a period of Twelve (12) months.

CONTENTS

Section No	Page
CONTENTS	
1. INTRODUCTION.....	3
2. SCOPE OF WORKS.....	4
3. BACKGROUND.....	8
4. COMPLIANCE AND STANDARDS.....	9
5. TERMS AND CONDITIONS.....	13



1. INTRODUCTION

The relentless attacks on personnel and vandalism of business-critical infrastructure at the TRIM Operating Division within the Central Corridor have resulted in operational disruptions. The frequency of these disruptions has increased in recent years and is now affecting the rest of Transnet's operational value chain.

1.1 Purpose of the document

- 1.1.1. Given the high level of losses associated with theft and vandalism, TRIM intends to implement a Rail Network Protection Services (RNPS) contract in the Central Corridor to reduce attacks on personnel, theft, vandalism of critical infrastructure, assets, etc. The Rail Network Protection Services (RNPS) shall provide for the 5 elements of the Security Management Life Cycle (Deter, Deny, Delay, Detect, and Detain) through integrated security solutions.
- 1.1.2. This Scope of Work (SOW) provides a clear appreciation of the functional requirements of the Rail Network Protection Services (RNPS) in the Central Corridor.

1.2. Primary objective and intended outcome of the Rail Network Protection Services (RNPS).

RNPS is a security approach in which the customer procures security services from Security Service Providers (SSPs) by specifying how those services should be rendered.

- 1.2.1. The approach of prescribing the security services required provides a clear indication of the resources that TRIM needs to be deployed for adequate protection of the sites.
- 1.2.2. The security services requirements are also prescribed to ensure uninterrupted security services and compliance.

1.3. Key Performance Indicators (KPIs) and Primary objectives of the Rail Network Protection Services (RNPS)

- 1.3.1. The performance of the SSPs will be closely monitored and non-performance shall lead to contract termination as detailed in the Master Services Agreement (MSA).
- 1.3.2. The primary objective of the Rail Network Protection Services (RNPS) is to achieve the outcomes in Table 1.

KPI	KPI Measure
Train Cancellations (due to Security Incidents)	Reduction of Slot Cancellations
Number Of Incidents theft and vandalism <i>Security Incident Management System (SIMA)</i>	Reduction of Overhead Traction Equipment (OHE) incidents
	Reduction of Signal cable incidents
	Reduction in Vandalism: Relay Room & Substation
	Reduction of Electrical cable incidents
	Reduction of Telecoms cables incidents
Minute Delays - <i>SIMA</i>	Reduction of Delays due to Security incidents
Length Of Cable - <i>SIMA</i>	Reduce length of cables and the associated replacement cost
Perway - <i>SIMA</i>	Reduction of Perway equipment incidents

Table 1 – KPIs and objectives of the RNPS.

1.4. Current Situation

- 1.4.1 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.
- 1.4.2 Infrastructure (Operational yards, depots, Operational bays, OHE, 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.).



- 1.4.3 Assets [Condition Assessment System (CAS), locomotives, wagons, railway line, rails, pendrol springs and other rail fastenings, locomotive batteries, tarpaulins, containers, signalling, point machines, etc.].
- 1.4.4 Commodity (Example, Chrome, manganese, sugar, wood, automotive, fuel, diesel, coal, etc.).
- 1.4.5 There are also other related security issues below which have an adverse impact on rail operations in the Central Corridor.
 - 1.4.5.1 Security Officer Management and supervision (Collusion, lack of supervision, etc.).
 - 1.4.5.2 Illegal occupation of the Rail reserve (Highly densified with encroachment, dilapidated buildings along the sections, etc.)
 - 1.4.5.3 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).

1.5 Implementation summary

The bidding company shall deploy the TRIM-prescribed physical security resources from contract inception to ensure that the entire corridor is secured from day one of the contract.

2. SCOPE OF WORKS

- 2.1** 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.

2.1.1. 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.

2.1.2. 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.

2.1.3. 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.

2.1.4. 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.

2.1.5. Defend/Retain 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.

2.2 Community engagement

2.2.1 The bidding company 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 include to the following:

- 2.2.1.1 Engage community stakeholders and establish partnerships with them.
- 2.2.1.2 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.
- 2.2.1.3 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.
- 2.2.1.4 Minimum 2 community engagements per quarter for the duration of the contract.

2.3 Law Enforcement Agencies

2.3.1 The bidding company shall provide a plan to interface with 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 security challenges in the Central Corridor. The plan shall include but not be limited to, the following:

- 2.3.1.1 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.
- 2.3.1.2 How to improve existing cooperation, coordination, and strengthen information sharing with Law Enforcement agencies.
- 2.3.1.3 How the bidding company shall conduct data analysis and a further plan on how to execute joint operations with other relevant stakeholders.

2.4 Physical resources required

- 2.4.1 The bidding company shall deploy the resources listed in Table 2.
- 2.4.2 Detailed deployment per Depot will be contained in the SLA.

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	76	90	166
Crime Prevention Vehicle, Single Cab (2 x 4) with vehicle tracking, at 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 (4 x 4) with vehicle tracking, at 10 000km pm)	12	17	17

Intervention Task Team Vehicle, Single Cab (2 x 4) with vehicle tracking, at 7000km per month	6	6	6
Intervention Task Team Leader /Driver Armed Grade C	6	6	12
Intervention Task Team Armed Crew Grade C	6	6	12
Crime Prevention Motorbikes	11	13	13
Crime Prevention Motorbike Rider Armed Grade C	11	13	24
Multi-rotor Drone Team	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	1
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 shutdown October 2026)			
Grade "C" - Unarmed Dayshift (Foot patrollers)	56	56	112
Crime Prevention Armed Driver Grade C	10	10	20
Crime Prevention Armed Crew Grade C	10	10	20
Crime Prevention Vehicle, Single Cab (2 x 4) with vehicle tracking, at 2 000km pm)	5	0	5
Multi-rotor Drone Team	2	0	2
11 x Days Shutdown (Second shutdown February 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	10	10	20
Crime Prevention Vehicle Single Cab (2 x 4) with vehicle tracking, at 2 000km pm)	5	0	5
Multi-rotor Drone Team	2	0	2

Table 2 - Physical security resources.

NOTE:

- Same motorbikes and vehicles will be used during day and night shifts.

2.4.3 TRIM schedules two shutdowns of 11 days each within identified sections of the corridor to carry out maintenance and repairs on the railway infrastructure. The bidding company shall provide an estimate for 2 annual shutdowns in the Central Corridor over a 12-month period.

2.4.4 Shutdown details:

2.4.4.1 TRIM schedules two shutdowns of 11 days each within identified sections of the corridor to carry out maintenance and repairs on the railway infrastructure. The bidding company shall provide a quote for 2 annual shutdowns in the Central Corridor over a 12-month period.

2.4.4.2 The table below illustrates the composition of a **multi-rotor drone team**.

PSIRA Grade "C" qualified Pilot x 1
A licensed pilot must be qualified UAS with the required skills and licenses
Support Crew [Armed Grade C] x 1
Safety Boots + Reflective Jackets

Bulletproof jacket level 3
Firearm .9mm + spare mag [min 15 rounds]
Vehicle – Single Cab 2.0L + Canopy (5 000km incl.) (24 hrs.)
08-hour shifts
Flashlight (e.g., Maglite 5 Cell or Similar 100-meter beam)
Rotar wing drone –minimum 8 kms range
Communication device - Two-way radio [PTT or similar technology with tracking]
Drone batteries (min 2) last 60 min each and are sufficient for a shift, either have sufficient or have a charging unit that must last 8 hours for a shift
Camera resolution: minimum X9 optical zoom, IP67 rating
Day and night camera with thermal functionality, minimum 12 MP

2.4.4.3 The table below illustrates the composition of a **Crime Prevention Team**.

Grade "C" (Armed) Driver x 1
Grade "C" (Armed) Crew x 1
Safety Boots + Reflective Jackets
Single Cab (2 x 4) with 10000 kms with vehicle tracking
Firearm 9mm (24 hrs. basis) spare magazine and 15 rounds
Bulletproof level 3
Flashlight (e.g., Maglite 5 C Cell or LED Similar) 100M Beam
Pepper Spray
Handcuffs – cuff -cable ties
Communication device - Two-way radio [PTT or similar technology with tracking]
Responsible for line patrols and Foot patroller support

2.4.4.4 The table below illustrates the composition of a **Tactical Team**.

Grade "B" (Armed) Driver x 1
Grade "C" (Armed) Crew x 2
Safety Boots + Reflective Jackets
Double Cab (4 x 4) with 10000 kms with vehicle tracking
Firearm 9mm + 2 magazines [15-round capacity]
Rifle .223 + 2 magazines [30-round capacity]
Bulletproof level 3
Flashlight (e.g., Maglite 5 C Cell or LED Similar) 100M Beam
Pepper Spray
Handcuffs – cuff -cable ties

Communication device - Two-way radio [PTT or similar technology with tracking]
Responsible for joint operations with TRIM and Law Enforcement, conducting ambush and disruptive operations.

2.4.4.5 The table below illustrates the composition of an **Intervention Task Team**.

Grade "C" (Armed) Driver x 1
Grade "C" (Armed) Crew x 1
Safety Boots + Reflective Jackets
Single Cab (2 x 4) with 7000 kms with vehicle tracking
Firearm 9mm + 2 magazines [15-round capacity]
Bulletproof level 3
Flashlight (e.g., Maglite 5 C Cell or LED Similar) 100M Beam
Pepper Spray
Handcuffs – cuff -cable ties
Communication device - Two-way radio [PTT or similar technology with tracking]
Responsible for crime prevention support (substations and relay room) and Stopper Groups at possible escape routes

3. BACKGROUND

- 3.1 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.
- 3.2 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 transported by rail.
- 3.3 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.
- 3.4 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:
- 3.4.1 Cluster 1 yards and lines (Sentrarrand, Natalspruit, Leeuhof, Sasolburg).
 - 3.4.2 Cluster 2 yards and lines (Elandsfontein, Mariesshoop, Springdale, Kaalfontein, Pretcon, Capital Park, Watloo, Greenview).
 - 3.4.3 Cluster 3 yards and lines (Potchefstroom, Klerksdorp, Krugersdorp, Mafikeng).
- 3.5 The Central Corridor has critical infrastructure below.
- 3.5.1 Length of the rail network – 2818 Kilometers (km)
 - 3.5.2 Total traction Sub = 58 (24 sites have existing technology) (34 no tech)
 - 3.5.3 Total distribution Sub = 41 (1 site has existing technology) (40 no Tech)
 - 3.5.4 Total relay room = 107 (25 sites have existing technology) (82 No Tech)

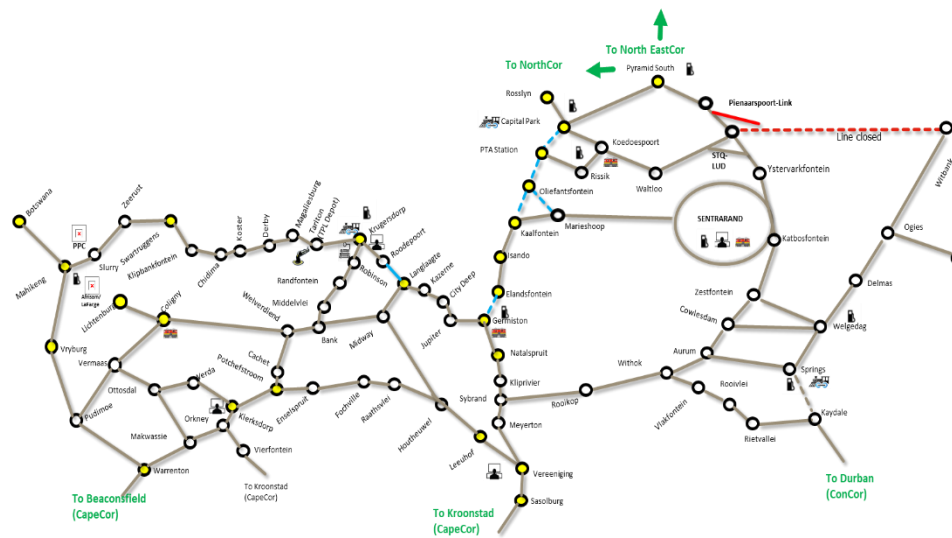


Provision of Rail Network Protection Services (RNPS) to Transnet Rail Infrastructure Manager (TRIM) within the Central Corridor for a period of Twelve (12) months.

3.5.5 Depots= 3

3.5.6 Yards= 35 (11 sites have existing technology)

3.6 The Central Corridor is illustrated on the map below:



4. COMPLIANCE AND STANDARDS

4.1. The bidding company shall submit the following documents as mandatory returnable documents. Compliance with all applicable legislation shall be at the SSP's cost. The bidding company shall be liable for any breach by any one or more of its security officers, employees, servants, 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.

N.B: All submitted documents and certificates must be valid on the closing date and time of the bid.

4.1.1. The bidding company 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 bid closing date and time.

4.1.2. The bidding company 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).

4.1.3. The bidding company 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).

4.1.4. The bidding company shall submit a letter of compliance from the Security Industry Provident Fund. The letter of compliance shall not have any outstanding amounts.

4.1.5. The bidding company 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.

4.1.6. The bidding company 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.

4.1.7. 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.

- 4.1.8. The bidding company shall submit a valid and signed Letter of good standing from PSIRA. The letter of good standing shall be on PSIRA letterhead.
- 4.1.9. The bidding company shall submit a signed Letter of Good Standing from the Compensation fund for Occupational Injuries and Diseases Act (COIDA).
- 4.1.10. The bidding company's security personnel must be registered with PSIRA. The bidding company shall submit valid PSIRA registration certificates (Minimum Grade C) of at least Five (5) security officers currently employed by the bidding company to prove compliance.
- 4.1.11. The bidding company's security personnel who are required to use firearms shall have SAPS firearm competency certificate. The bidding company 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.
- 4.1.12. Valid Remote Operator Certificate (ROC) + Operations Specifications (OpSpecs) page showing authorized operations.
- 4.1.13. BVLOS authorization on OpSpecs or signed undertaking to obtain BVLOS approval prior to commencement as condition precedent, with SACAA consultation proof.
- 4.1.14. Valid ICASA radio frequency spectrum license or ICASA type approval certificates for proposed RPA models.
- 4.1.15. The bidder shall submit two hundred and eighty (280) firearm licences owned by the company and available for deployment.

4.2. Compliance with statutes

- 4.2.1. The Bidder 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 Bidder's cost.
 - 4.2.1.1. PSIRA Act (56 of 2001), as amended;
 - 4.2.1.2. Private Security Industry Levies Act, (23 of 2002);
 - 4.2.1.3. National Key Points Act (102 of 1980), as amended;
 - 4.2.1.4. Basic Conditions of Employment Act (75 of 1997);
 - 4.2.1.5. Compensation for Occupational Injuries and Diseases Act (130 of 1993), as amended;
 - 4.2.1.6. Provincial ordinances and laws and municipality by-laws including all relevant regulations promulgated;
 - 4.2.1.7. The Occupational Health and Safety Act (83 of 1993);
 - 4.2.1.8. Protection of Personal Information Act (4 of 2013);
 - 4.2.1.9. Firearms Control Act, (60 of 2000), as amended;
 - 4.2.1.10. Criminal Procedure Act (51 of 1977);
 - 4.2.1.11. Control of Access to Public Premises and Vehicles Act (53 of 1985), as amended;
 - 4.2.1.12. Codes of Good Practice embodied in the Broad Based Black Economic Empowerment Act (53 of 2003);
 - 4.2.1.13. Independent Communications Authority of South Africa Act (13 of 2000), as amended;
 - 4.2.1.14. Legal Succession to the South African Transport Services Act (9 of 1989);
 - 4.2.1.15. Income Tax Act (52 of 1962);
 - 4.2.1.16. Value-added Tax Act (89 of 1991);
 - 4.2.1.17. Trespass Act (6 of 59)
 - 4.2.1.18. Matters Amendment Act (18 of 2015);
 - 4.2.1.19. Any other legislation and regulations and/or in-house specific policies, procedures guidelines that govern some of the Client's sites; and
 - 4.2.1.20. Any other regulatory obligation such as the Railway Safety Regulator (RSR) Act (16 of 2002).
 - 4.2.1.21. The South African Civil Aviation Authority (SACAA).

4.3. Shutdown costs

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



Provision of Rail Network Protection Services (RNPS) to Transnet Rail Infrastructure Manager (TRIM) within the Central Corridor for a period of Twelve (12) months.

- 4.3.2. 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 11 days per shutdown.
- 4.3.3. The bidding company shall provide a quote for 2 annual shutdowns in the Central Corridor over a 12-month period.
- 4.3.4. Accordingly, the SSP shall, for the duration of the shutdown period, deploy additional security personnel over and above the baseline establishment. The additional officers and the deployment plan shall be demobilized upon the resumption of normal rail operations at the end of each shutdown period.
- 4.3.5. Remuneration for the additional security officers deployed during shutdown periods shall be compensated separately in accordance with the rates tendered in the Pricing Schedule under "Once-off Shutdown pricing". No claim for standby or overtime shall be entertained unless prior written approval has been obtained from TRIM.

4.4. Experience and Track Record

- 4.4.1. TRIM is calling for proposals from the SSPs with demonstrable experience in the provision of security services ---in the Rail Infrastructure, National Key Poit, and Government Institutions.
- 4.4.2. It is a requirement that the bidder should have a minimum of five (05) years in the provision of security services. To demonstrate experience in the delivery of the required security services, the bidding company shall supply a minimum of 3 reference letters from the bidding company's past or present clients.
- 4.4.3. To demonstrate experience in the delivery of the required security services, the bidding company shall supply a minimum of 3 reference letters from the bidding company's past or present clients.
- 4.4.4. Each reference letter shall be accompanied by a corresponding contract award letter. Any reference letter and contract award letter that do not correspond will be deemed non-responsive and not considered during evaluation.
- 4.4.5. The reference letters shall meet the requirements below:
 - 4.4.5.1. Be on the referee's client's letterhead;
 - 4.4.5.2. Be signed off by the bidding company's client
 - 4.4.5.3. Be dated;
 - 4.4.5.4. Provide contactable references;
 - 4.4.5.5. Provide a brief description of security services provided by the bidding company; and
 - 4.4.5.6. State the contract period (Start date and end date).

NOTE: TRIM reserves the right to contact references for verification.

4.5 Service Level Agreements (SLAs) - A detailed SLA will be provided to the successful bidder as part of the MSA.

4.6 Reporting and Documentation

- 4.6.1 The SSP shall be required to capture incidents, provide trend analysis, provide high-level reporting in line with TRIM's requirements.
- 4.6.2 All incidents shall be accompanied by incident (First Information of Crime) and investigation reports.

4.7 Proof of Presence

- 4.7.1 The bidding company shall demonstrate operational presence within the TRIM Central Corridor comprising of Gauteng and Northwest provinces.
- 4.7.2 The bidding company shall submit the following for every province listed in 4.7.1 to validate operational presence in the Central Corridor:
 - 4.7.2.1 Proof of ownership(s) and/or lease agreement(s) of premises.
 - 4.7.2.2 Physical addresses of decentralised armoury.

4.8 Transitional/Takeover phase

- 4.8.1 To facilitate operational continuity during the transition period, the successful service provider ('New SSP) shall have the discretionary right, but not the obligation, to engage existing deployed personnel from the incumbent SSP with employment opportunity.
- 4.8.2 Such engagement is strictly contingent upon the incumbent SSP's written confirmation that the relevant personnel are not required for other contracted sites and that the incumbent SSP's employment obligations have been duly satisfied or assumed.
- 4.8.3 The new SSP retains the sole prerogative to determine the selection, terms, and remuneration of such personnel, who shall be employed by the new SSP in its own capacity, thereby ensuring that any employment-related liabilities, disputes, or claims arising from such engagement rest solely with the new SSP.
- 4.8.4 Transnet shall not be liable for any employment claims, benefits, or disputes between the new SSP and these transitional personnel, provided that the new SSP indemnifies Transnet against such claims.
- 4.8.5 The SSP will be responsible to secure the corridor from contract commencement date.
- 4.8.6 The bidder shall submit a commitment later confirming its undertaking to deploy the required resources on the contract commencement date.
- 4.8.7 Bidders who fail to deploy one hundred percent (100%) of the required resources will forfeit points during desktop evaluation.

4.9. Implementation requirements

- 4.9.1 The service provider shall have working relationships with different stakeholders which include but are not limited to communities, industry, farmers, traditional leaders, Community Policing Forums, Law Enforcement Agencies, Prosecuting Authorities, etc, or establish such relations.
- 4.9.2 The SSP shall attend the daily, weekly and monthly meetings at all levels.
- 4.9.3 The SSP shall be proactive in the prevention and detection of incidents, respond to incidents and emergencies.
- 4.9.4 The SSP shall have the capability of covert operations (ability to do information gathering and analysis) and investigations.

4.10. Polygraph testing

- 4.10.1 TRIM reserves the right to require polygraph/vetting examinations for any SSP personnel deployed on the RNPS contract, where there is reasonable suspicion of involvement in criminal activity, misconduct, policy violations, or loss/damage to employer assets. The SSP shall comply with such requests within 5 working days of written instruction from TRIM.
- 4.10.2 Polygraph tests shall be conducted by a reputable, PSIRA-registered polygraph examiner independent of the SSP.
- 4.10.3 Testing shall be limited to matters directly related to the contract, site security, theft, vandalism, cable theft, and breach of confidentiality.
- 4.10.4 Results shall be treated as confidential and shared only with TRIM and the SSP's Senior Management.
- 4.10.5 All costs associated with the polygraph examination, including examiner fees, travel, and administrative charges, shall be for the account of the SSP.
- 4.10.6 TRIM shall not be liable for any costs arising from polygraph testing under this clause.
- 4.10.7 Should an employee fail or refuse to undergo a polygraph test or should results indicate deception related to contract-related offenses, TRIM may instruct the SSP to immediately remove such personnel from site and replace them at no additional cost to TRIM.
- 4.10.8 Communication must be proactive, transparent, and timely. Regular updates must be provided without the need for repeated follow-ups.
- 4.10.9 Results must be submitted within five (5) working days.

4.10.10 Members undergoing the polygraph process must be removed from the line until the process is fully completed.

4.11 baseline risk assessment

- 4.11.1 The SSP shall conduct a service-specific security risk assessment for the TRIM sites.
- 4.11.2 The successful bidder (appointed SSP) shall conduct a risk assessment and rate the likelihood of incidents, events, or accidents, and the consequences of incidents, events, or accidents at all sites
 - 4.11.2.1 Such ratings shall be recorded in the Individual Agreement not later than the first month of the Agreement.
 - 4.11.2.2 These risk ratings will remain constant during the term of this Agreement unless a new risk assessment has been conducted that results in the rating changing. Any such change must be endorsed by the Controlling Officer and communicated to the client in writing, with the necessary amendments being made to the Individual Agreement and signed off by both Parties.
- 4.11.3 The SSP shall provide firearms, ammunition, and bulletproof vests where applicable and based on the risk assessment that will be conducted.
- 4.11.4 The service provider will conduct continuous Risk Assessments to ensure the integrity of security personnel.

4.12 Health and safety

- 4.12.1 The Safety, Health, and Environment (SHE) Specification, 37 (2) Mandatory Agreement, E7/1 Working next to railway lines and health and safety questionnaire shall be submitted as part of the tender deliverables and to ensure compliance with Health and Safety Act, Act 85 of 1993, other applicable legislation and standards.
- 4.12.2 The Service Providers are required to provide First Aid Training to all their security officers, and keep the training up to date, as per the safety regulations and Laws.
- 4.12.3 The Service Providers shall undergo regular OHTE [Overhead Traction Equipment] safety awareness, including ground equipment. All Service Providers are required to have a 'Safety File' and keep it up to date.

5. TERMS AND CONDITIONS

- 5.1.** Contractual obligations – See the full details on the Master Services Agreement (MSA) (**Annexure A**).
- 5.2.** The SSPs are required to provide a signed acceptance of the Scope of Works.
- 5.3.** The SSPs are required to provide a detailed project schedule based on the scope of works.
- 5.4.** Non-disclosure and Confidentiality Agreement – Refer to **Annexure C**.
- 5.5.** Service Level Agreements (SLAs)
 - 5.5.1. A detailed SLA will be provided to the successful bidder as part of the signing of the MSA.
- 5.6.** Reporting and Documentation
 - 5.6.1. The SSP shall be required to capture incidents, provide trend analysis, provide high-level reporting in line with TRIM's requirements.
 - 5.6.2. All incidents shall be accompanied by an incident report (First Information of Crime), investigation reports and an SAPS-generated case number.

6. Obligations of the SSP

- 6.1 The required security services would safeguard personnel, assets, and properties that cover a large area and various locations within the corridor, including, among other things, the TRIM major installation sites.
- 6.2 The SSPs will be responsible for contract management of their personnel and providing TRIM with daily deployment of security resources at all locations. This will form part of the daily "Posting Sheets". Dishonesty and inaccurate reporting would



constitute a severe breach of contract and may lead to termination.

- 6.3 All alarm triggers from existing TRIM security systems require the SSP to dispatch the response team quickly to the site. A quick response and backup are crucial to ensure that assets and personnel are not unnecessarily put at risk in the absence of effective contingency plans.
- 6.4 TRIM will not entertain any deployment deviations provided to the SSPs if they (the SSPs) have failed to secure the site. In this case, any negligence by the SSP will result in claims being initiated under the Master Service Agreement for poor service delivery.
- 6.5 The SSPs shall be required to attend all reported security incidents, secure crime scenes, investigate crime breaches within the area of responsibility, which includes the integrity tests (polygraph testing) by a registered service provider, and report the crime to TRIM as well as to the South African Police Service (SAPS) within 24 hours.
- 6.6 Failure to report incidents to the South African Police Service (SAPS) will be regarded as a breach of contract. Furthermore, the SSP is required to provide testimony during court proceedings as part of the contract requirements and expectations without additional remuneration.