



Security Plan for TRANS ESCRAVOS PIPELINE (TEP) & TRANS RAMOS PIPELINE (TRP)

Date issued: 2022-05-31



Foreword

The Security Plan is developed and maintained for Shell facilities or activities by the responsible Corporate Security Manager (CSM) or Asset Protection Manager (APM). It identifies the key assets and processes, associated risks and (planned) mitigation measures. The document is owned by the respective Site / Activity Manager who remains accountable for all risk management activity.

Template version May 2022

Version Control

CONFIDENTIAL

The Security Plan (SP) will be reviewed and updated in conjunction with the Security Management Register (SMR) and in line with the outcome of the Security Risk Assessment (SRA) review by the responsible Corporate Security Manager or Asset Protection Manager. If any updates are required due to changes in threat or materiality, a new version of the Security Plan will be issued with the key changes logged below.

| SP Issued | Author | Approved By | Approved By | |
|-------------|--|--|---|---------|
| 2023-03-28 | Essiene McLean Stanley | Eke Omoruyi | Uche Ojiako | |
| | Area Security Adviser, Pipeline West | Pipeline Security Manager | Head of Availability & ROW Management | |
| | | | | |
| Review Date | Reviewed By | Reviewed By | Reviewed By | Changes |
| 2023-01-25 | Essiene McLean Stanley Area Security Adviser, Pipeline West | Eke Omoruyi Pipeline Security Manager | Uche Ojiakor Head, Pipeline RoW & Surveillance | 1 |
| | | | | 2 |
| | | | | 3 |
| | | | | 4 |
| | | | | 5 |
| YYYY-MM-DD | Enter Author name | Enter Approver name | Enter Reviewer name | 1 |
| | | | | 2 |
| | | | | 3 |
| | | | | 4 |
| | | | | 5 |
| YYYY-MM-DD | Enter Author name | Enter Approver name | Enter Reviewer name | 1 |
| | | | | 2 |
| | | | | 3 |
| | | | | 4 |
| | | | | 5 |
| YYYY-MM-DD | Enter Author name | Enter Approver name | Enter Reviewer name | 1 |
| | | | | 2 |
| | | | | 3 |
| | | | | 4 |
| | | | | 5 |

TABLE OF CONTENTS*

| | |
|--|----|
| 1. Executive Summary..... | 5 |
| 2. Facility/Activity Overview | 6 |
| 2.1 Facility/Activity Description | 6 |
| 3. Security Organisation | 7 |
| 3.1 Overview..... | 7 |
| 3.2 Organisation Chart..... | 7 |
| 4. Security Risks | 9 |
| 4.1 Facility/Activity Risk Summary | 9 |
| 5. Security Risk Mitigation Plan | 10 |
| 5.1 Overview..... | 10 |
| 5.2 Physical & Technical Security | 10 |
| 5.3 Security Procedures..... | 13 |
| 6. Training and Exercises | 15 |
| 6.1 Training Requirements..... | 15 |
| 6.2 Exercises & Drills | 16 |
| Appendix 1: Facility Drawings..... | 17 |
| Appendix 2: Key Contacts* | 18 |
| Appendix 3: Security System Details | 19 |
| Appendix 4: Security Measures for EACH SOL | 20 |
| Appendix 5: Security RASCI Chart..... | 23 |

Table of Figures

| | |
|--|----|
| Figure 1: Security Plan Summary | 5 |
| Figure 2: Security Plan Facility/Activity* | 6 |
| Figure 3: Security Organisation Chart* | 7 |
| Figure 4: Facility/Activity Security Risk Summary..... | 9 |
| Figure 5: Physical/Technical Security Risk Mitigations | 11 |
| Figure 6: Training Requirements per Role* | 15 |
| Figure 7: Security Exercises & Drills* | 16 |
| Figure 8: Facility/Activity Drawing* | 17 |
| Figure 9: Key Contacts..... | 18 |
| Figure 10: Security System Details* | 19 |
| Figure 11: SOL Security Procedures* | 20 |
| Figure 12: Security RASCI Chart | 23 |

1. EXECUTIVE SUMMARY

Overview*

Risk Environment*

Figure 1: Security Plan Summary

| Key Facility/Operations Summary | Key Threats (Threat Levels) |
|---|---|
| <p>The Trans-Ramos Pipeline (TRP), with length of about 74.32km and the Trans Escravos Pipeline (TEP) with length is about 45km both traverse the swamp operational areas of SPDC West.</p> <p>The TRP consists of the Beneside delivery line which ties into the Opukushi-brass creek trunk line at the brass creek manifold station. From Brass creek the TRP connects the Ogbotobo tie-in line manifold where the Ogbotobo delivery lines ties into it, the TRP from here passes through Agge & Aghoro where it crosses the Ramos river and finally terminates at the Forcados terminal (FOT).</p> <p>The TEP stretches from Yokri Northbank from the Forcados River through Obotobo, Sokobolo to Escravos Beach where it crosses the Escravos River to Saghara, and then onto Otumara</p> | <ul style="list-style-type: none"> ▪ Criminality (7) ▪ Organized crime (9) |
| Key Risk Scenarios | Key Mitigations |
| <ul style="list-style-type: none"> ▪ Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks ▪ Installation of illegal connection on the pipeline to siphon crude ▪ Vandalization of the manifold/theft of components | <ul style="list-style-type: none"> ▪ Intelligence ▪ Surveillance ▪ Sea/Bush watchers ▪ GSAs (static and mobile patrols) ▪ PSS. |

2. FACILITY/ACTIVITY OVERVIEW

2.1 Facility/Activity Description

The scope of this Security Plan is the protection of the facility/activity detailed in Figure 2 below:

Figure 2: Security Plan Facility/Activity*

| Category | Description |
|-------------------------------------|--|
| Line of Business* | Upstream |
| Facility/Activity Overview** | <p>Trans Ramos Pipeline (TRP) commonly called the TRP is about 74.32km long. It is located within Delta and Bayelsa States and traverses several LGAs, towns and communities</p> <p>The Trans Escravos Pipeline (TEP) whose entire length is about 18km, traverses the swamp area consisting of SPDC Mining licences covering OMLs 40, and 43.</p> |
| Materiality** | <p>The TRP evacuates oil from Benisede, Tunu, Opukushi, Brass Creek, Ogbotobo, Agge Aghoro, Odimodi to Forcados Terminal. The system currently has a gross evacuation capacity of ca.476, 137MMbpd.</p> <p>The TRP system is a strategic and economic component in the Western Oil production chain as the network availability impacts directly on production and on the overall unit operating cost.</p> <p>The TEP evacuates oil produced from parts of Northern swamp which covers Opuama, Outumara, Saghara, Escravos Beach, Yokri and Forcados North Bank fields' productions. TEP discharges into the Trans Forcados pipeline (TFP) at Forcados River Manifold. The system currently has a gross evacuation capacity of ca. 280,000MMbpd.</p> <p>The Assets covered by the SPDC West pipeline network include manifolds, tie-in Manifolds, and pipelines connecting the Manifolds which are; Opukushi MF, Brass Creek Tie-in MF, Benisede MF, Forcados Terminal.</p> <p>The Manifolds which are; Otumara MF, Saghara Tie-in MF, Escravos Tie-in MF, Yokri Tie-in MF, Forcados North Bank MF, Forcados River</p> <p>The TEP include manifold, tie-in Manifolds, and pipelines connecting the Manifolds which are; Otumara MF, Saghara Tie-in MF, Escravos Tie-in MF, Yokri Tie-in MF, Forcados North Bank MF, Forcados River MF.</p> |

A drawing showing the layout and main components of the facility can be found in Appendix 1.

3. SECURITY ORGANISATION

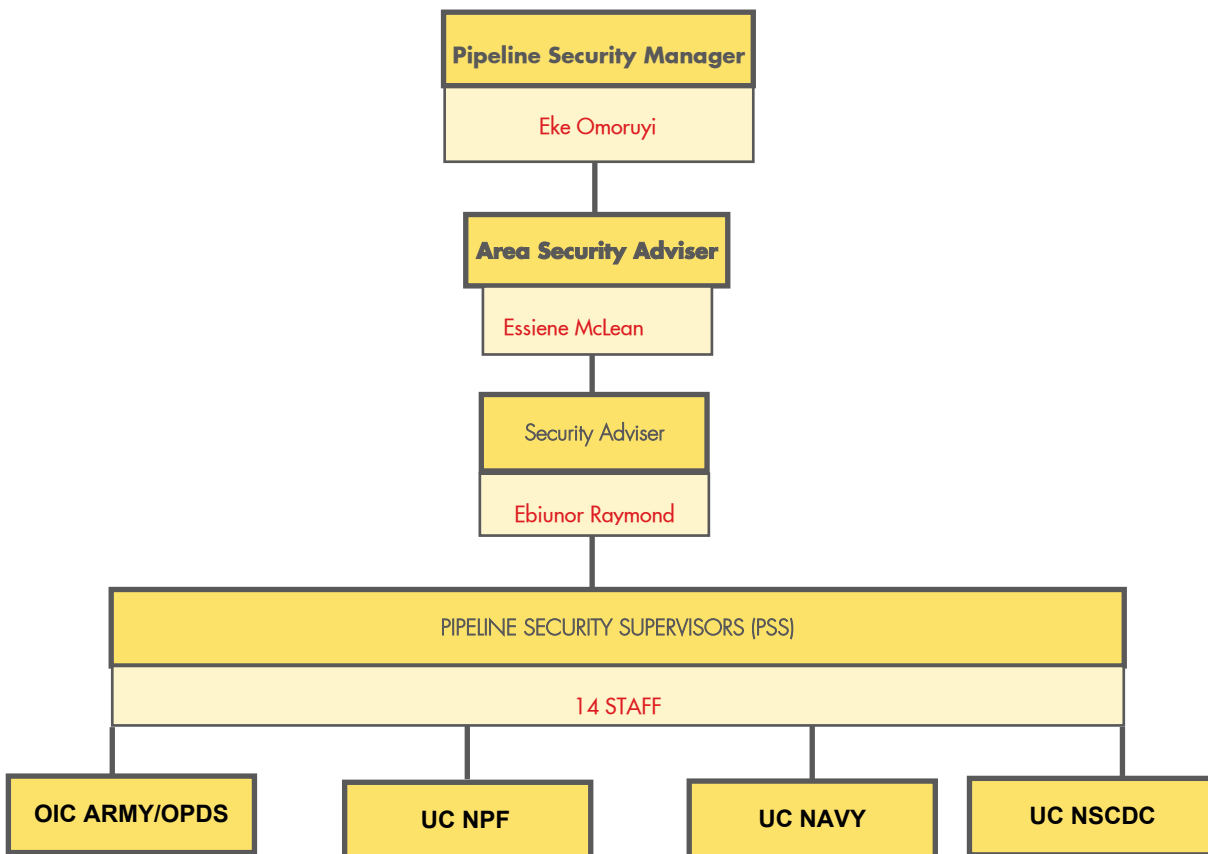
3.1 Overview

The local security team consists of 253 Government Security Agents; 14 Pipelines Security Supervisors; 1 Security Adviser; 1 Area Security Adviser; and 1 Pipelines Security Manager providing day-to-day (24/7) operational security for this asset. The Pipeline Security Supervisors are responsible for security in various locations across the network and reports to the SA/ASA, who in turn reports to the PSM who is ultimately accountable for security of the facility.

3.2 Organisation Chart

A security organisation chart is provided in Figure 3*;

Figure 3: Security Organisation Chart*



Contact information for the above roles, as well as related security functions and external response agencies can be found in Appendix 2.

| Role | Name | Contact Details (e.g. landline, mobile phone, email) |
|--------------------------------------|------------------------|--|
| Pipeline Security Manager | Eke Omoruyi | 08070344174 |
| Area Security Adviser | Essiene McLean Stanley | 08070310705 |
| Security Adviser | Ebiunor Raymond | 08070316782 |
| Security Adviser, Special Operations | Nwofube Awele | 08070322279 |

4. SECURITY RISKS

4.1 Facility/Activity Risk Summary

Figure 4 summarises the key risk scenarios from the latest facility/activity Security Risk Assessment (SRA), which is documented in full in the Stature application. These risks are the focus of the security risk management activity for the site, with related mitigation measures described in Section 5 of the Security Risk Mitigation Plan.

Extract the security risks from the SRA ('Key Risks Identified' section) and include within Figure 4. Allocate a numerical risk number in the first column as this will be cross-referenced with the security mitigations in section 5.

Figure 4: Facility/Activity Security Risk Summary

| Risk # | Asset Activity | Threat Category | Scenario Description | Risk Rating |
|--------|--|--------------------------------|--|-------------|
| 1 | TEP: 20" Otumara-Escravos | Criminality Organised crime | Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks Installation of illegal connection on the pipeline to siphon crude | 5 |
| 2 | TEP: 20" Escravos-Forcados Terminal | Criminality Organised crime | Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks Installation of illegal connection on the pipeline to siphon crude | 5 |
| 3 | TEP: Delivery lines | Criminality Organised crime | Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks Installation of illegal connection on the pipeline to siphon crude | 4 |
| 4 | TEP: Manifolds | Criminality Organised crime | Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks Installation of illegal connection on the pipeline to siphon crude | 4 |
| 5 | TRP: 20" Opukushi-Brass creek | Criminality Organised crime | Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks Installation of illegal connection on the pipeline to siphon crude | 5 |
| 6 | TRP: 24" Brass creek-Forcados Terminal | Criminality Organised crime | Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks Installation of illegal connection on the pipeline to siphon crude | 5 |
| 7 | TRP: Delivery lines | Criminality Organised crime | Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks Installation of illegal connection on the pipeline to siphon crude | 4 |
| 8 | TRP: Manifolds | Criminality Organised crime | Sabotage on the line through drill hole, hacksaw cut, fire and IED attacks Installation of illegal connection on the pipeline to siphon crude | 4 |

5. SECURITY RISK MITIGATION PLAN

5.1 Overview

The security risks identified in Section 4 will be mitigated to ALARP level via a combination of physical, technical and procedural security measures. A risk mitigation plan is provided in the following figures, with a summary of the physical, technical and procedural mitigation measures that are in place for each of the identified risks. Further information on specific security systems (such as vendor details, installation and end-of-life dates, and support contracts in place) can be found in Appendix 3.

5.2 Physical & Technical Security

Guidance – Physical/Technical Security:

- **Security Measure:** add/delete as appropriate.
- **Coverage:** briefly specify where each measure is deployed and what parts of the asset are covered. e.g. video surveillance = full coverage of the building perimeter, all entry points and car parks.
- **Capability:** specify key capabilities of each technology, e.g. video surveillance = 24/7 imaging, video analytics-based target detection and tracking, 30 days recording, etc.
- **Risk Scenarios Mitigated:** insert the numerical risk reference for all scenarios in Section 4 that each measure is intended to help mitigate.
- Include hyperlinks to Appendix 3 (Security System Detail) where applicable.

Figure 5: Physical/Technical Security Risk Mitigations

| Security Measure | Coverage | Capability | Risk Number (Risk Scenarios Mitigated) |
|---|---|---|---|
| A. Detection Measures | | | |
| Overfly (aerial surveillance) | Coverage of entire network at least ones every week | Provide realtime information and pictures that aid timely response to third party interference on the facility | 1, 2, 3, 4, 5, 6, 7, 8 |
| RoW Surveillance | At least 12 hours coverage of entire network daily | Early detection of third party interference on the facility | 1, 2, 3, 4, 5, 6, 7, 8 |
| Intelligence | Multi-level, internal and external intelligence sources | Provide information for timely response to prevent third party interference on the facility | 1, 2, 3, 4, 5, 6, 7, 8 |
| GSA Patrols | 24/7 RoW patrols across the network | Early detection of third party interference on the facility | 1, 2, 3, 4, 5, 6, 7, 8 |
| Sea/Bush Watchers | 24/7 coverage of key sections of the network | Provide additional level of protection to the facility due to local community knowledge, supports via local intelligence. Not fully deployed across the network | 1, 2, 3, 4, 5, 6, 7, 8 |
| B. Delay Measures | | | |
| Perimeter Fencing and installation of gates at manifolds | All manifolds fenced and gated to prevent unauthorised access | Mitigates unauthorised access to the facility. A number of fences and gates require upgrade works | 4, 8 |
| Burial of pipelines | Entire pipeline on the network buried at different depths | Largely increases the time it takes criminals to have access to the facility but some sections usually exposed by erosion. | 1, 2, 3, 4, 5, 6, 7, 8 |

| C. Response Measures | | | |
|-------------------------------|--|---|------------------------|
| Communication Systems | GSM communications amongst Security Supervisors and pipeline security leadership team | Do not support 24/7 communication due to network unavailability in some remote locations | 1, 2, 3, 4, 5, 6, 7, 8 |
| Security Management System | The Security Operations Centre (SOC) supports team's monitoring and response functions | Full integration of components pending the deployment of satellite communication gadgets across the network | 1, 2, 3, 4, 5, 6, 7, 8 |
| GSA Response | 24/7 coverage across the network | 24/7 response across most of the network except difficult terrains | 1, 2, 3, 4, 5, 6, 7, 8 |
| Pipeline Security Supervisors | Over 70% coverage, coordinating GSA and other resources utilisation | Below 100% supervision. A few camps not fully manned | 1, 2, 3, 4, 5, 6, 7, 8 |

5.3 Security Procedures

Guidance – Security Procedures:

- **Incident Response Procedures:** list the key procedures in place with a hyperlink to the SharePoint file. These could include for example: Activist Protest / Blockade, Perimeter Intrusion, Bomb Threat, Armed Attack etc.
- **Security Operating Levels:** include site-specific SOLs in Appendix 4.
- **SOPs / Guard Force Instructions:** list those in place with a hyperlink to a local (facility/activity) file. These could include for example; key control, routine patrols, access control and visitor policy, weapons storage, etc.
- **Security Awareness Campaigns:** identify any regular campaigns and provide a hyperlink to the briefing material. This could include for example 'Think Secure', 'Active Shooter', etc.

| Category | Procedure (Hyperlink) | Risk Number (Risk Scenarios Mitigated) |
|--|--|---|
| Incident Response Procedures | <ul style="list-style-type: none"> ▪ Encountering theft of crude oil In progress ▪ Encountering leak on the pipeline right of way (RoW) ▪ Encountering suspicious ground signs on the RoW | 1, 2, 3, 4, 5, 6, 7, 8 |
| Security Operating Levels | <ul style="list-style-type: none"> ▪ Link to appendix 4 | 1, 2, 3, 4, 5, 6, 7, 8 |
| Standard Operating Procedure/Guard Force Instruction | <ul style="list-style-type: none"> ▪ GSA operating procedures and techniques ▪ Communication in security operations ▪ VPSHR briefing | 1, 2, 3, 4, 5, 6, 7, 8 |
| Security Awareness Campaigns | <ul style="list-style-type: none"> ▪ Security briefing to crews deployed for routine and emergency maintenance works on the facility | 1, 2, 3, 4, 5, 6, 7, 8 |

6. TRAINING AND EXERCISES

6.1 Training Requirements

All security personnel must be given the appropriate training to ensure that they can fulfil their role. Based on a training needs analyses, the requirements for each role are shown in Figure 6 below.

Figure 6: Training Requirements per Role *

| Role | Training Requirements & Description |
|-------------------------|---|
| Shift Supervisor (PSS) | <ul style="list-style-type: none"> The Area Security Adviser will implement and maintain the relevant training programmes at the Facility. These programmes will be specifically dependent upon the Security requirements for the individual Facility and the risks identified within the Security Risk Assessment. Detailed training records are to be retained at each Facility. Such identified relevant security training may be sponsored by the Asset and or Security. <p>Training include:</p> <ul style="list-style-type: none"> Facility Orientation PSS Pre-Deployment Training Security Risk Management and Intelligence Course Security Reporting Tecnigues Voluntary Principles On Security And Human Rights (VPSHR) |
| Guard Team Member (GSA) | <p>All Guards should undergo Initial Training which should include, but is not limited to:</p> <ul style="list-style-type: none"> Voluntary Principles On Security And Human Rights Use of Force guidelines. |
| Other (surveillance) | <p>All surveillance Guards should undergo Initial Training which should include, but is not limited to:</p> <ol style="list-style-type: none"> Surveillance guards pre-engagement training Incident reporting techniques |

6.2 Exercises & Drills

Security exercises and drills are an important method to validate and improve the security risk mitigation capability. The following exercises are undertaken for this facility/activity.

Figure 7: Security Exercises & Drills*

| Test/ Exercise | Description | Frequency |
|----------------|--|-----------|
| | Pipeline security operation is real time in nature and continuous improvement mindset is propogated through the spread of lessons learnt | |

Figure 8: Facility/Activity Drawing*



APPENDIX 2: KEY CONTACTS*

Figure 9: Key Contacts

| Role | Name | Contact Details (e.g. landline, mobile phone, email) |
|--------------------------------------|---------------------------|--|
| Pipeline Security Manager | Eke Omoruyi | 08070324139 |
| Area Security Adviser | Essiene McLean Stanley | 08070310705 |
| Security Adviser | Ebiunor Raymond | 08070316782 |
| Security Adviser, Special Operations | Nwofude Awele | 08070322279 |
| PSS Aghoro (Ndoro Junction) Pipeline | Felix Orido | 08070316315 |
| PSS Aghoro (Ndoro Junction) Pipeline | Ogbegu Victor Ogbe | 08070316315 |
| PSS Agge Pipeline | Daufa Aladi Patrick | 08070316315 |
| PSS Agge Pipeline | Femi Ayebusiwa | 08070316315 |
| PSS Brass Creek Pipeline | Endurance Tubon | 08070316301 |
| PSS Brass Creek Pipeline | Wakama Tamunosiki Promise | 08070316301 |
| PSS Tamogbene Pipeline | Boma Tolofari | 08070316319 |
| PSS Tamogbene Pipeline | Okwazu Augustine | 08070316319 |
| PSS Escravos Pipeline | Ekrake Oghale Jerry | 08070316317 |
| PSS Escravos Pipeline | Ifeanyin Jeffery Uchekwe | 08070316317 |
| PSS Ugbuengungun/Otumara Pipeline | Okwari Balentyn | 08070316318 |
| PSS Ugbuengungun/Otumara Pipeline | Alfred Adakole Iduh | 08070316318 |
| PSS Yokri/Northbank Pipeline | Obinna Douglas Ede | 08070316579 |
| PSS Yokri/Northbank Pipeline | Dennis Fiberesima Atoku | 08070316579 |





APPENDIX 3: SECURITY SYSTEM DETAILS


Figure 10: Security System Details*

| Area | System Details |
|--|---|
| 1. SYSTEM TYPE (VIDEO SURVEILLANCE / ACCESS CONTROL / INTRUSION DETECTION / OTHER) | |
| System Type* | Video Surveillance System / Access Control System / Intrusion Detection System / Other |
| Overflight (aerial surveillance) | Operators with an intimate knowledge of the ground spot signs of illegal activities on the pipeline RoW |

APPENDIX 4: SECURITY MEASURES FOR EACH SOL

Figure 11: SOL Security Procedures*

| Threat Level | Security Operating Level | Security Measures / Procedures |
|---|---|---|
|  EXTREME |  BLACK | <p>Indications</p> <ul style="list-style-type: none"> Evacuate/lockdown Security incident(s) occurring that are directly impacting Shell Operations or its staff. <p>Actions</p> <ul style="list-style-type: none"> General Implement Facility Shut Down Plan. Evacuate all staff if possible, remainder to Safe Haven Emergency Response Armed Response Team deployed-reserve brought to Immediate Notice To Move(NTM) Travel Security authorized moves only or as per travel SOL. Patrolling Continuous Patrols of facility & Perimeter Access Control Authorization List to be produced and only staff on the list to be granted access to Facility and Critical locations. No Contractor's admitted . All Access Gates and Building entry's locked(keys to be held locally). Parking No parking within Facility. Search 100% Random search of personnel. 100%vehicles fully searched. Loss Prevention All stores secured, no stores to be issued/received Communications Full Situation Reports to be sent every 30 mins. |
|  HIGH |  RED | <p>Indications</p> <ul style="list-style-type: none"> Evacuated Security Security incidents resulting in loss of life occurring frequently in the area. Government Security forces engaged in Operations near to Shell Operations This alert level may be activated on receipt of a specific threat and for a limited period of time. <p>Actions</p> <ul style="list-style-type: none"> General Implement Facility Shut Down Plan. Evacuate all staff if possible, remainder to Safe Haven Emergency Response Armed Response Team deployed-reserve brought to Immediate Notice To Move(NTM) Travel Security authorized moves only or as per travel SOL. |

| | | |
|---|--------------|--|
| | | <ul style="list-style-type: none"> ▪ Patrolling Continuous Patrols of facility & Perimeter ▪ Access Control Authorization List to be produced and only staff on the list to be granted access to Facility and Critical locations. No Contractor's admitted . All Access Gates and Building entry's locked(keys to be held locally). ▪ Parking No parking within Facility. ▪ Search 100% Random search of personnel. 100%vehicles fully searched. ▪ Loss Prevention All stores secured, no stores to be issued/received ▪ Communications Full Situation Reports to be sent every 30 mins. |
|  | <p>AMBER</p> | <p>Indications</p> <ul style="list-style-type: none"> ▪ Major security incidents occur infrequently in the area ▪ Increased and visible security forces activity ▪ Non-specific threats against Operations & Staff ▪ Potential for civil unrest ▪ Embassies issue periodic warden messages or warnings ▪ Threats and actions against other IOC's in area <p>Actions</p> <ul style="list-style-type: none"> ▪ General Minimum Manning at Facility Safe Haven to be identified and hardened ▪ Emergency Response Security Response Team available - 2 mins NTM ▪ Travel Security Escorts to be used for persons at risk(PAR)in line with Journey Management plan. Movement restricted to Security approved routes. Daylight movement only(Waiver required for nighttime movement) Other Travels as per Travel SOL. ▪ Patrolling Random Patrols of facility & Perimeter(Minimum 1 per hour) ▪ Access Control Establish Forward Checkpoint at ECP ▪ Staff 100% visual (Technical if available) check of all entries to Facility and at entrance to identified restricted areas ▪ Visitors/Contractors ID Confirmation & Issuance of visitors passes ▪ Parking Parking in identified locations only ▪ Search 50% Random search of personnel. 100% Random search of vehicle boots. 1/25 vehicles fully searched. Full Search personnel & vehicle search for cause. ▪ Loss Prevention Manned Guarding at stores locations ▪ Key Control |

| | | |
|---|--------------|---|
| | | <p>100% accounting and Key Register to be inspected weekly</p> <ul style="list-style-type: none"> ▪ Firearms Law Enforcement/ Government Security Forces Only ▪ Communications Radio comms check to all manned locations every hour. Twice Daily comms check to Control Room Alternate comms check twice daily to Control Room |
|  <p>LOW</p> | <p>GREEN</p> | <p>Indications</p> <ul style="list-style-type: none"> ▪ No restrictions ▪ Base Line Security ▪ Little or no violent crime ▪ Armed aggression events are rare ▪ Security Forces are in control <p>Actions</p> <p>General Global Security Standards Baseline Security Performance Criteria implemented</p> <p>Emergency Response Security Response Team available-5mins Notice To Move(NTM)</p> <p>Travel Day/Night movement in line with Journey Management. As per Travel SOL.</p> <p>Patrolling Random Patrols of facility & Perimeter(Minimum 1 per 2 hours)</p> <p>Access Control</p> <p>Staff 100% visual check of all entries to Facility Visitors/Contractors ID Confirmation & Issuance of visitors passes</p> <p>Search 1/50 Random search of personnel. 1/50 Random search of vehicle boots. 1/100 vehicles fully searched. Full Search personnel & vehicle search for cause.</p> <p>Loss Prevention No Random Search of Vehicles departing the Facility. Property Removal Authorization controls Implemented</p> <p>Key Control 100% accounting and Key Register to be inspected monthly</p> <p>Firearms No Firearms to be permitted in the Facility</p> <p>Communications Radio comms check to all manned locations every 2 hours Daily comms check to Control Room Firearms to be permitted in the Facility</p> |

APPENDIX 5: SECURITY RASCI CHART

This describes the agreed 'Responsibilities', 'Accountabilities', 'Supportive', 'Consulted' and 'Informed' functions of management with security responsibilities.

Figure 12: Security RASCI Chart

| Security RASCI | CCH | BM/SM | CSM | APM/SFP | RSM |
|---|-----|-------|-----|---------|-----|
| Country Threat Assessment | A | I | C | I | C |
| Country Security Operating Levels | A | I | R | I | S |
| Security Assurance | A | A | S | R | S |
| Country Security Plan & Review | A | I | R | I | S |
| Security Awareness Training | I | I | R | S | S |
| Security Liaison | C | I | A/R | I | S |
| Promote VPSHR | A | S | S | R | I |
| EC Security | I | I | S | S | C |
| Security Expense | I | A/R | S | S | S |
| Develop & Maintain Contingency Plans | A | A | S | R | S |
| Site/Facility Security Risk Assessments | I | A | R | R | I |
| Site/Facility Security Plans | I | A | S | R | I |

TRP

TRP (ZONE 13) DEPLOYMENTS

CURRENT DEPLOYMENTS

- Agge – Porta Cabin, 2 MPVs, 5 Patrol boats, 25 GSAs (15 from 5 Batt; 10 from NSCDC Delta)
- Ndoro Junction – Houseboat, 2 MPVs, 3 Patrol Boats, 27 GSA (Sec 1)
- Brass Creek – Porta cabin, 2 MPVs, 2 patrol boats, 30 GSAs (15 from 5 Batt; 15 from NSCDC)
- Tamogbene – Houseboat, 2 MPVs, 2 Patrol Boats, 39 GSAs (343 Art Reg)

The map shows the coastline of Zone 13, Bayelsa State, Nigeria. Key locations include Forcados Terminal, KP 29, Ogbotobo FS, Brass Creek MF, Benisede MF, Excal (3rd Party), Tunu FS, and Opukushi MF. A green line indicates the route or boundary, with various icons representing different types of vessels and equipment deployed at each location.

