| Section | Requirements | weighting | Tenderer's self assessment Score as per evaluation criteria (1 to 5) | TFR Score (1 to 5) | Weighted Score | Proof/ Reference / Referral / Experience / Certificate |
|---|---|---|---|---|---|---|
| 1 | Cyber security compromise and impact assessment of the recent cyber-attack incident within the Operational Technology (OT) ecosystem and underlying infrastructure | | | | | |
| 1.1 | **Assessment of current processes:** The purpose of this requirement is to determine the adequacy of the Transnet's current processes in the identification of OT ecosystem security threats and vulnerabilities, response to cyber security incidents and management involvement in the identification and incident response processes. | | | | | |
| 1.2 | During this phase, the service provider will be required to remediate all active vulnerabilities and threats identified in the environment. | | | | | |
| 1.3 | Activities to be carried out will be guided by the recommendations made by the service provider in the compromise and impact assessment. | | | | | |
| 2 | Threat hunting to establish the cyber security posture, level of vulnerability, active threats and exposure to cyber threats within OT ecosystem; | | | | | |
| 2.1 | The purpose is to test the following components of the OT ecosystem and underlying infrastructure from the internal network:□ | | | | | |
| 2.1.1 | Operating systems | | | | | |
| 2.1.2 | Databases | | | | | |
| 2.2 | Findings report to describe all the issues in ecosystems with remedial actions to resolve the issues. The report should contain the elements including but not limited to the following: | | | | | |
| 2.2.1 | Information security patches | | | | | |
| 2.2.2 | Database and Operating systems | | | | | |
| 2.2.3 | Network settings | | | | | |
| 2.2.4 | Systems Security | | | | | |
| 2.2.5 | Security policies review | | | | | |
| 2.2.6 | Remote access | | | | | |
| 2.2.7 | Current Cyber Security threats that could exploit the OT ecosystem | | | | | |
| 2.2.8 | Hostname | | | | | |
| 2.2.9 | IP Address | | | | | |
| 2.2.10 | MAC Address | | | | | |
| 2.2.11 | Corridor, Depot, Yard, Corporate office Location | | | | | |
| 2.2.12 | List of checks done | | | | | |
| 2.2.13 | List of security issues identified | | | | | |
| 2.2.14 | Description of security issues | | | | | |
| 2.2.15 | Risk rating or severity | | | | | |
| 2.2.16 | Category of Risk: Critical / High / Medium / Low | | | | | |
| 2.2.17 | Methodology/Test cases used in assessment | | | | | |
| 2.2.18 | Illustration of the test cases | | | | **60** | |
| 2.2.19 | Applicable screenshots | | | | | |
| 2.2.20 | Analysis of vulnerabilities and issues of concern | | | | | |
| 2.2.21 | Likely impact on business | | | | | |
| 2.2.22 | Recommendations for corrective action | | | | | |
| 3 | An assessment of the risk exposure introduced by convergence of Information Technology (IT) and OT ecosystem. | | | | | |
| 4 | Penetration tests to assess the effectiveness of existing security controls | | | | | |
| 4,1 | The purpose of this phase is for the service provider to try and connect to the OT ecosystem internal network and exploit systems in a controlled manner. Findings and testing during this phase must include but must not be limited to the following: | | | | | |
| 4.1.1 | Current Cyber Security threats that could exploit the Transnet OT ecosystem. | | | | | |
| 4.1.2 | Emerging Cyber Security threats that could exploit the Transnet OT ecosystem. | | | | | |
| 4.1.3 | Exploitation of found vulnerabilities that are exploitable. | | | | | |
| 4.1.4 | Suggestions for mitigation | | | | | |
| 4.1.5 | Report and recommendations as well implementation of the security controls to prevent reoccurrence of a similar cyber attack. | | | | | |
| 5 | To make recommendations and implementation of the corrective measures and security controls: | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 5.1 | Threat and Vulnerability Assessment report | | | | | |
| 5.2 | Threat and Vulnerability severity ratings and detailed remediation recommendations | | | | | |
| 5.3 | Implementation of remedial actions on active threats and vulnerabilities | | | | | |
| 6 | To develop a cyber security capability roadmap (technology/OEM agnostic) required to improve the security posture to ensure safe, secure, reliable, and resilient OT ecosystem in line with TFR's zero trust principle. | | | | | |
| 7 | The service provider should provide the high-level plan/methodology that is going to be used to perform the scope of work and clearly demonstrate on how the deliveries will be achieved. The phases involved in typical security assessment project are: | | | | | |
| 7.1 | · Planning and Preparation | | | | | |
| 7.2 | · Assessment | | | | | |
| 7.3 | · Reporting | | | | | |
| 7.4 | · Recommendation and Remediation | | | | | |
| 7.5 | · Capability roadmap | | | | | |