C4-AES-05-L&E (Addendum-01)

<table>
<tr><th>Sl. No.</th><th>Part/Section</th><th>Clause No.</th><th>Original Bid Condition</th><th>Revised Bid Condition</th></tr>
<tr><td>1</td><td>Part-1, Section - III Evaluation and Qualification Criteria (EQC)</td><td>1.1.1</td><td>Personnel
The Bidder must demonstrate that it has the personnel for the key positions that meet the following requirements:
<table><tr><th>No.</th><th>Position</th><th>Qualification</th><th>Nos.</th><th>Total Work Experience (Minimum number of years)</th><th>Experience in Similar Works (Minimum number of years)</th></tr><tr><td>1</td><td>Project Manager (PM) – Lifts & Escalators</td><td>Graduate in Electrical/ Mechanical Engineering</td><td>1</td><td>15</td><td>10</td></tr><tr><td>2</td><td>Deputy Project Manager (DPM) - Lifts</td><td>Graduate in Electrical/ Mechanical Engineering</td><td>1</td><td>10</td><td>5</td></tr><tr><td>3</td><td>Deputy Project Manager (DPM) - Escalator</td><td>Graduate in Electrical/ Mechanical Engineering</td><td>1</td><td>10</td><td>5</td></tr><tr><td>4</td><td>Design Engineer – Lifts</td><td>Graduate in Electrical/ Mechanical Engineering</td><td>1</td><td>5</td><td>3</td></tr><tr><td>5</td><td>Design Engineer – Escalators</td><td>Graduate in Electrical/ Mechanical Engineering</td><td>1</td><td>5</td><td>3</td></tr><tr><td>6</td><td>Interface Manager (to be posted at Chennai site from design stage till commissioning of last station)</td><td>Graduate in Electrical/ Mechanical Engineering</td><td>1</td><td>8</td><td>5</td></tr><tr><td>7</td><td>Project Engineer – Lifts</td><td>Graduate in Electrical/ Mechanical Engineering</td><td>2</td><td>5</td><td>3</td></tr><tr><td>8</td><td>Project Engineer – Escalators</td><td>Graduate in Electrical/ Mechanical Engineering</td><td>2</td><td>5</td><td>3</td></tr></table></td><td>Deleted (This Condition is shifted to Part-2 / Employers Requirement)</td></tr>
<tr><td>2</td><td>Part-1, Section - III Evaluation and Qualification Criteria (EQC)</td><td>1.1.2</td><td>The Bidder shall demonstrate that it has the key equipment required for construction, installation, testing and commissioning:
<table><tr><th>No.</th><th>Equipment Type and Characteristics</th><th>Minimum Number Required</th><th>Remarks</th></tr><tr><td>1</td><td>Crane (Minimum 10 Ton)</td><td>2 Nos</td><td rowspan="5">In case of equipment which are older than 10 years from bid submission date, Fitness Certificates obtained from OEM for the respective equipment should be submitted.</td></tr><tr><td>2</td><td>Truck (10 Ton)</td><td>2 Nos</td></tr><tr><td>3</td><td>Forklift</td><td>2 Nos for each station</td></tr><tr><td>4</td><td>Extendable Ladder Trolley</td><td>2 Nos for each station</td></tr><tr><td>5</td><td>Generator (40kVA)</td><td>1 No. for each station</td></tr></table></td><td>Deleted (This Condition is shifted to Part-2 / Employers Requirement)</td></tr>
<tr><td>3</td><td>Part-1, Section - III Evaluation and Qualification Criteria (EQC)</td><td>2.4.2 (b)</td><td>1. If the bidder is from foreign country, they should have an international experience of supplying at least 40 similar Heavy- Duty Lifts and/or 80 Escalators to minimum one country outside his country of origin.

2. The bidder (Indian Member in case of JV/Consortium) should have their own established maintenance facilities in India at least for the past five (5) years and should have an average annual maintenance portfolio of Minimum 100 Nos of Lifts and 190 Nos of Escalator for Metro/ Airport/Sub-urban Railways/Railways/Tech Park building for a period of five (05) years with At least 20 Nos. of Lifts and 35 Nos. of Escalators every year between 1st Jan 2017 and the bid submission deadline. For this purpose, the Lifts and/or Escalators which are under DLP, shall also be considered.</td><td>1. If the bidder is from foreign country, they should have an international experience of supplying at least 40 similar Heavy-Duty Lifts and 80 Escalators to minimum one country outside his country of origin.

2. The bidder (Indian Member in case of JV/Consortium) should have their own established annual maintenance facilities in India at least for the past five (5) years and should have an average annual maintenance portfolio of atleast 20 Lifts and 35 Escalators for every year between 1st Jan 2017 and 31st December 2021. For this purpose, the Lifts and/or Escalators which are under DLP, shall also be considered.</td></tr>
<tr><td>4</td><td>Part-1, Section - III Evaluation and Qualification Criteria (EQC)</td><td>2.5</td><td>Subcontractors/manufacturers</td><td>Deleted (This Condition is shifted to Part-2 / Employers Requirement)</td></tr>
<tr><td>5</td><td>Part-1, Section - III Evaluation and Qualification Criteria (EQC)</td><td>2.6</td><td>Preference to Local Suppliers/Preference to ‘Make In India’ Policy:</td><td>Deleted</td></tr>
<tr><td>6</td><td>Part 1 Section IV Bidding Forms</td><td>4.3</td><td>Price Centre C1:
Comprehensive Annual Maintenance (CAMC) Services for Stage 1 stations during Defect Notification period of 2 Years. (To be carry forwarded from BOQ ‘CAMC’) - % Breakup - 1%

Price Centre C2:
Comprehensive Annual Maintenance (CAMC) Services for Stage 2 stations during Defect Notification period of 2 Years. (To be carry forwarded from BOQ ‘CAMC’) - % Breakup - 1%

No changes in other Price Centres.</td><td>% Breakup shall be read as
Price Centre C1:
Comprehensive Annual Maintenance (CAMC) Services for Stage 1 stations during Defect Notification period of 2 Years. (To be carry forwarded from BOQ ‘CAMC’) - % Breakup - 1.3%

Price Centre C2:
Comprehensive Annual Maintenance (CAMC) Services for Stage 2 stations during Defect Notification period of 2 Years. (To be carry forwarded from BOQ ‘CAMC’) - % Breakup - 0.7%

No changes in other Price Centres.</td></tr>
<tr><td>7</td><td>Part 2: Section VI-A: General Specification</td><td>4.5</td><td>Enterprise Resource Planning</td><td>Deleted.</td></tr>
<tr><td>8</td><td>Part-1, Section - IV Bidding Forms</td><td>5.13</td><td>Bidders to propose this form for each of the following items in line with Cl. 2.5 of EQC.

Other details remains same.</td><td>Bidders to propose this form for each of the following items in line with Cl. No. 12.20 of Part-2, Section VI-A General Specification.
Other details remains same.</td></tr>
<tr><td>9</td><td>Part-1, Section - IV Bidding Forms</td><td>12</td><td>-</td><td><u>New Item Added</u>

<u>Format for Parent Company Guarantee & Parent Company Undertaking.</u>

<u>Refer Attachment 4 enclosed.</u></td></tr>
<tr><td>10</td><td>Part-1, Section - IV Bidding Forms</td><td>4.3.2</td><td>-</td><td><u>New Item Added (Note 3)</u>
Separate individual cost details for both Regenerative Drive and Without Regenerative Drive for the Vertical rise 6 meter and above to be submitted. However, this shall not be part of tender evaluation. This is to facilitate CMRL to decide to provide Regenerative drive in case if it is required.</td></tr>
</table>

<table>
<tr><th colspan="5">C4-AES-05-L&E (Addendum-01)</th></tr>
<tr><th>Sl. No.</th><th>Part/Section</th><th>Clause No.</th><th>Original Bid Condition</th><th>Revised Bid Condition</th></tr>
<tr><td>11</td><td>BOQ</td><td>BOQ</td><td>BOQ1, BOQ2, BOQ3, BOQ4</td><td>Refer revised BOQ1, BOQ2, BOQ3, BOQ4.</td></tr>
<tr><td>12</td><td>Part 2: Section VI-A: General Specification</td><td>6.1</td><td>Project Management Information System (PMIS)</td><td>Refer Attachment 7 enclosed.</td></tr>
<tr><td>13</td><td>Part 2: Section VI-A: General Specification</td><td>7.2</td><td>Key Personnel
7.2.1 The Contractor’s Staffing Proposal shall include the minimum Personnel for the Key Positions (Key Personnel) as stated in the Section lll, Eligibility and Qualification Criteria, Part 1.

7.2.2 All the Key Personnel shall meet the Experience and Qualifications requirements appropriate to the nature of the work as defined in the Appendix 15 Section III, Part 1 of this document. The Contractor shall submit the proposal with the details of the Key Personnel as defined, to the Engineer for his review and NONO</td><td>Key Personnel
7.2.1 The Contractor’s Staffing Proposal shall include the minimum Personnel for the Key Positions (Key Personnel) as stated in the <u>Attachment-03</u> enclosed.

7.2.2 All the Key Personnel shall meet the Experience and Qualifications requirements appropriate to the nature of the work as defined in the <u>Attachment-03</u> enclosed of this document. The Contractor shall submit the proposal with the details of the Key Personnel as defined, to the Engineer for his review and NONO</td></tr>
<tr><td>14</td><td>Part 2: Section VI-A: General Specification</td><td>7.2.3</td><td>-</td><td><u>New Item Added</u>
<u>Personnel: Refer Attachment-03 enclosed.</u></td></tr>
<tr><td>15</td><td>Part 2: Section VI-A: General Specification</td><td>7.3</td><td>-</td><td><u>New Item Added</u>
<u>Equipment</u>
The Bidder shall demonstrate that it has the key equipment required for construction, installation, testing and commissioning:
<table><tr><th>No.</th><th>Equipment Type and Characteristics</th><th>Minimum Number Required</th><th>Remarks</th></tr><tr><td>1</td><td>Crane (Minimum 10 Ton)</td><td>2 Nos</td><td rowspan="5">In case of equipment which are older than 10 years from bid submission date, Fitness Certificates obtained from OEM for the respective equipment should be submitted.</td></tr><tr><td>2</td><td>Truck (10 Ton)</td><td>2 Nos</td></tr><tr><td>3</td><td>Forklift</td><td>2 Nos for each station</td></tr><tr><td>4</td><td>Extendable Ladder Trolley</td><td>2 Nos for each station</td></tr><tr><td>5</td><td>Generator (40kVA)</td><td>1 No. for each station</td></tr></table>The Bidder shall provide further details of these items of equipment using ‘Form EQU’ in Section IV, Bidding Forms</td></tr>
<tr><td>16</td><td>Part 2: Section VI-A: General Specification</td><td>12.20</td><td>-</td><td><u>New Item Added</u>
Subcontractors/manufacturers for the following major items of supply or services must meet the following minimum criteria, herein listed for that item:
<u>Refer Attachment 6 enclosed.</u></td></tr>
<tr><td>17</td><td>Part 2: Employer’s Requirements
Section VI-B: Technical Specifications: Lifts/Escalators</td><td>2.4.1 (n)</td><td>The contractor shall comply with cyber security policy /guidelines for the web-based software applications and its infrastructure to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks, and technologies as per the latest CEA (Cyber Security in Power Sector) Guidelines 2021 issued by Government of India.</td><td>Tender Condition Prevails.

Also, <u>Refer Attachment-01 & Attachment-02 enclosed.</u></td></tr>
<tr><td>18</td><td>Part 2 Section VIB Techncial Specification-Lifts/Escalators</td><td>4.2.2</td><td>Isoceraunic level: Average 30 thunderstorm days per year as per IS 2309:1989</td><td>Isoceraunic level: As per IS 2309:1989/ EN 62305 latest version.</td></tr>
<tr><td>19</td><td>Part 2: Employer’s Requirements
Section VI-B: Technical Specifications: Lifts</td><td>5.1 A, Sl.No. 3</td><td>For 13 Passenger 1000 kg the car size mentioned as 1600mm (W) x 1400mm (D) for shaft size 2500mm (W) x 1900mm (D) for single side opening lift. But the shaft size 2500mm (W) x 2100mm (D) mentioned in contract for double side opening type lift (through car), hence the car size could be 1500mm (W) x 1500mm (D) for this shaft size.</td><td>Car inside area shall be min. 2.24 Sq. m and shall comply with Clause No. 4.14 of Part-2 Technical Specifications which can be accomodated within the given shaft dimensions. Sizes can be finalised during design stage.</td></tr>
<tr><td>20</td><td>Part 2: Employer’s Requirements
Section VI-B: Technical Specifications: Lifts</td><td>5.1 B, Sl.No. 2</td><td>Car Size : 2000mm (W) x 1800mm (D) x 2300mm (H) or 1600mm (W) x 2400mm (D) x 2300mm (H)</td><td>Car inside area shall be min. 3.6 Sq. m and shall comply with Clause No. 4.14 of Part-2 Technical Specifications which can be accomodated within the given shaft dimensions. Sizes can be finalised during design stage.</td></tr>
<tr><td>21</td><td>Part 2: Employer’s Requirements
Section VI-B: Technical Specifications: Lifts</td><td>5.2.8</td><td>Lift car shall have minimum internal dimensions of 1600 mm (Width) X 1400 mm (Depth) for carrying the rated load of 1000 kg/ 13 passengers Lifts. The false ceiling ….. on a wheel chair.</td><td>Car inside area shall be min. 2.24 Sq. m and shall comply with Clause No. 4.14 of Part-2 Technical Specifications which can be accomodated within the given shaft dimensions. Sizes can be finalised during design stage. The false ceiling ….. on a wheel chair.</td></tr>
<tr><td>22</td><td>Part 2: Employer’s Requirements
Section VI-B: Technical Specifications: Lifts</td><td>5.2.9</td><td>Lift car shall have minimum internal dimension (Width x Depth) 2000mm X 1800mm or 1600mm X 2400mm for carrying the rated load of 1800 kg/26 passenger Lifts. The false ceiling ….. on a wheel chair.</td><td>Car inside area shall be min. 3.6 Sq. m and shall comply with Clause No. 4.14 of Part-2 Technical Specifications which can be accomodated within the given shaft dimensions. Sizes can be finalised during design stage. The false ceiling ….. on a wheel chair.</td></tr>
<tr><td>23</td><td>Part 2: Employer’s Requirements
Section VI-B: Technical Specifications: Lifts</td><td>5.2.20 (g)</td><td>Provide the means for the control to reset Lift earthquake operation.</td><td>Provide the means for compliance to Seismic operation as per applicable codes & standards.</td></tr>
</table>

C4-AES-05-L&E (Addendum-01)				
Sl. No.	**Part/Section**	**Clause No.**	**Original Bid Condition**	**Revised Bid Condition**
24	Part 2: Employer's Requirements Section VI-B: Technical Specifications: Lifts	5.12	The Contractor shall provide a Lift inter-communication between the Lift Car, main control cubicle and SCR/EFO/OCC room consisting of master and slave stations	***Refer Sl.No. 6 (1), Annexure-D Interface Sheets of Appendix 16, Interface Management, General Specifications, Part-2 Employer's Requirements.***
25	Part 2: Employer's Requirements Section VI-B: Technical Specifications: Lifts	5.2.7	The gear less drive machine shall be mounted on guide rails accommodated within the Lift shaft. The power switch gear..... paramount importance. Lifts intended to be procured shall have a carrying capacity (rated load) of at least 1000kg/ 13passengers and 1800 Kg/26 passengers are defined in the Bid Document. The nominal speed for the Lifts shall be 1.0 m/s in either direction. For those lifts travel height from one landing to another landing is more than 15 meters, the nominal speed for Lifts shall be 1.5 m/s in either direction to be considered. Shaft enclosure shall be either RCC or Glass type structure or as per site conditions..... The contractor shall be responsible for any delay on this account.	***"The gear less drive machine shall be, mounted on guide rails/ accommodated within the Lift shaft". Without compromising on head room size & other safety parameters and all required beams & fixing arrangement shall be in the scope of L&E contractor.*** The power switch gear..... paramount importance. ***Lifts intended to be procured shall have a carrying capacity (rated load) of at least 1000kg/ 13passengers and 1800 Kg/26 passengers are defined in the Bid Document. The nominal speed for the Lifts shall be 1.0 m/s in either direction. Shaft enclosure shall be either RCC or Glass type structure or as per site conditions.....*** .The contractor shall be responsible for any delay on this account.
26	Part 2: Employer's Requirements Section VI-B: Technical Specifications: Lifts	5.8.8 ii (h)	Hand/Grip Rail - Scratch Resistant Stainless Steel	***Hand/Grip Rail - Stainless Steel Mirror finish***
27	Part 2: Employer's Requirements Section VI-B: Technical Specifications: Lifts	5.27.3 8.6.1 8.6.2	Proto type landing and car doors made of glass panels with stainless steel frame shall be pre-assembled in factory for inspection before delivery. One complete Lift shall be available for the commencement of witness testing after Contract Award. The selected Lifts shall be representative of their various types. A complete Lift system including traction drive system, in addition to the controller, Lift car enclosure, landing and car doors, protection devices and call fixtures shall be assembled on a test rig or inside a test tower to undergo a comprehensive running and functional testing in accordance with the accepted test specification to verify compliance with the Specification.	***A complete Lift system including traction drive system, in addition to the controller, Lift car enclosure, landing and car doors, protection devices and call fixtures shall be assembled on a test rig or inside a test tower at the Contractor's works to undergo a comprehensive running and functional testing in accordance with the accepted test specification to verify compliance with the Specification.***
28	Part 2 Section VIB Techncial Specification- Lifts	5.22.2	Fixed Cat Ladders shall be provided between the bottom landing and the pit floor by the Contractor as per the latest EN standard. The ladder shall be galvanized steel.	**Fixed Ladders** shall be provided between the bottom landing and the pit floor by the Contractor as per the latest EN standard. The ladder shall be galvanized steel.
29	Part 2 Section VIB Techncial Specification- Lifts	5.33	**Condition Based Monitoring for Lifts :** **Lifts:** a. Speed profile including constant monitoring of acceleration, top speed and deceleration and the optimum speed curves b. Floor level accuracy c. Incoming voltage and current d. Back up battery and UPS status e. Intercom and emergency phone line status f. Power usage g. Automatic Rescue Device Status h. Vibrations i. Rope/Belt Tension Balance j. Overheating of Motor k. Safety sensors status l. Limit switches status m. Pit water leakage status	**Condition Based Monitoring for Lifts :** **Lifts:** a. Floor level accuracy b. Incoming voltage and current c. Back up battery and UPS status d. Intercom and emergency phone line status e. Power usage f. Automatic Rescue Device Status g. Motor displacement status h. Rope/Belt Tension Balance i. Overheating of Motor j. Major Safety sensors status k. Pit Float sensor/switch status
30	Part 2 Section VIB Techncial Specification- Lifts	6.1.1	The design of each component shall achieve the minimum service life given below. The failure rate of the components shall not exceed 5%. Failure rate is defined as the number of failures (during the service life) divided by the total quantity of the components in one section. **S.No Lifts Service Life(in yr)** **1** Safety gear rope 15 **2** Governor 20 **3** Hoisting rope/Belt/Chain 15 **4** Contactors/Relays 10 **5** Traction Machine/Motor 20	The design of each component shall achieve the minimum service life given below. The failure rate of the components shall not exceed 5%. Failure rate is defined as the number of failures (during the service life) divided by the total quantity of the components in one section. **S.No Lifts Service Life(in yr)** **1** Safety gear rope 15 **2** Governor 20 **3** Hoisting rope/Belt/Chain *8* **4** Contactors/Relays 10 **5** Traction Machine/Motor 20 **6.** Car & Counterweight Guiderails including Brackets 30 **7.** Car & Counterweight Frame 30 **8.** Traction Machine Bearing & Diverter Wheel Bearing 1,10,000 operating hours
31	Part 2 Section VIB Techncial Specification- Lifts	5.3.3 (g)	The Lift machine shall be fitted with a manual emergency device capable of having the brake released by hand and requiring a constant effort to keep the brake open. In case of MRL lifts, the motor brake shall be able to be remotely (both electrical and manual) released outside the lift well.	The Lift machine shall be fitted with a manual emergency device capable of having the brake released by hand and requiring a constant effort to keep the brake open. ***The manual emergency device shall be handle operated. The handle should be robust and able to bear the human intervention. The termination of brake cable at handle of manual emergency device should be mechanically double secured and fail safe. Alternative arrangement (if any) proposed in compliance with the Codes and Standards of Lift will be evaluated during detailed design stage. The Employer's decision is final.***

C4-AES-05-L&E (Addendum-01)				
Sl. No.	**Part/Section**	**Clause No.**	**Original Bid Condition**	**Revised Bid Condition**
32	Part 2 Section VIB Techncial Specification- Lifts	5.4.1	At least Three (3) steel wire ropes or coated steel belts (min. 3 meeting the IS 15785 with min factor of safety 12) specially manufactured for Lift use shall be employed for the suspension of Lift car and Counterweight. The diameter/ dimension and specification of rope for the car and counterweight shall conform to latest version/ amendments of EN -81 and IS: 14665	***"Steel wire ropes or coated steel belts*** (meeting the IS 15785 with min factor of safety 12) specially manufactured for Lift use shall be employed for the suspension of Lift car and Counterweight. The diameter/ dimension and specification of rope for the car and counterweight shall conform to latest version/ amendments of EN -81 and IS: 14665"
33	Part 2 Section VIB Techncial Specification- Lifts	5.8.4 (a)	The car platform shall be constructed from cold rolled steel (spray galvanized) with stainless steel/ Granite stone finished flooring matches to the lift lobby floor finish/6mm Aluminum Chequered plate. The platform shall be designed on the basis of the rated load evenly distributed with a minimum safety factor of five (5).	The car platform shall be constructed from cold rolled steel***/ hot rolled steel*** (spray galvanized) with stainless steel/ Granite stone finished flooring matches to the lift lobby floor finish/6mm Aluminum Chequered plate. The platform shall be designed on the basis of the rated load evenly distributed with a minimum safety factor of five (5).
34	Part 2 Section VIB Techncial Specification- Lifts	5.16.2	Next Landing The car door fails to open in designated floor the controller should allow the Lift to go to safe lock mode as per EN81-20/50 against passenger safety.	***Deleted***
35	Part 2 Section VIB Techncial Specification- Lifts	5.18.7	Maintenance Access Panel (MAP) should preferably be located at Top landing floor level.	Maintenance Access Panel (MAP) should be located at ***Top Landing of the Lift shaft.*** .
36	Part 2 Section VIB Techncial Specification- Lifts	5.9.3	On “Without Attendant” mode, if no command is registered or due to some abnormality in Lift Safety circuit, after the expiry of a preset time interval of 10-30 seconds (Adjustable) the door shall re-open once for 30 seconds (Adjustable) to enable the passengers to exit and close after the set period. No changes in other Paragraphs.	On “Without Attendant” mode, if no command is registered or due to some abnormality in Lift Safety circuit, after the expiry of a preset time interval of 10-30 seconds (Adjustable) the door shall re-open to enable the passengers to exit and close after the set period. This will be reviewed and finalised during the design stage. No changes in other Paragraphs.
37	Part 2 Section VIB Techncial Specification- Lifts	5.8.10	**Last paragraph of the clause.** Work Light and Duplex 16A Plug Receptacle: Provide protected outlet inside car, on roof and bottom of car. Include on/off switch and lamp guard. A convenience outlet in car is required to facilitate ease of vacuuming cars during cleaning. It can be located in a locked service cabinet, in the car operating panel or the Cabin base.	**Last paragraph of the clause.** Work Light and Duplex 16A Plug Receptacle: Provide protected outlet inside car, on roof and bottom of car. Include on/off switch and lamp guard. It can be located in a locked service cabinet, in the car operating panel and the Cabin base. This will be reviewed and finalised during the design stage.
38	Part 2 Section VIB Techncial Specification- Lifts	5.15 (d)	**Second Line of the paragraph.** Hanger cover plates shall be made of galvanized steel	**Second Line of the paragraph shall be read as** Hanger cover plates shall be made of ***stainless*** steel
39	Part 2 Section VIB Techncial Specification- Lifts	5.25.7	Each Lift shall be provided with the following accessories: a) Two sets each of all necessary keys for the landing door, operating panel, etc. b) Four sets of maintenance barrier. c) One set of UPS unit maintenance kit.	Each Lift shall be provided with the following accessories: a) Two sets each of all necessary keys for the landing door, operating panel, etc. ***b) Two set of maintenance barrier per station (Considering maximum number of landings for 2 Lifts in that particular station)*** c) One set of UPS unit maintenance kit.
40	Part 2: Section VI-B: Technical Specifications: Lifts	5.10.2 (g)	**Last Line of the paragraph.** When the alarm button shall be pressed for 3 second, then automatically the command will go to intercom also.	**Last Line of the paragraph shall be read as** When the alarm button shall be pressed, then automatically the command will go to intercom also.
41	Part 2: Section VI-B: Technical Specifications: Lifts	5.15.1	The One (1) set of jumbo type of minimum size 50 x 50 mm hall call buttons shall be provided for each Lift at every floor served. The set of buttons shall be installed on the wall adjacent to each Lift landing. The face plate shall be made of scratch resistant stainless steel grade 304. The Stainless steel plate should be at least 3 mm thick and its mounting arrangement should have two Sunken Screws…..the illumination shall cease. The buttons should be permanently illuminated of dull illumination and on activation shall be bright illumination. Sizes and Finishes should be submitted by the Contractor to “Employer/Employer’s Representative” for review and finalization during detailed design phase.	The One (1) set of jumbo type of minimum size 50 x 50 mm hall call buttons shall be provided for each Lift at every floor served. The set of buttons shall be installed on the wall adjacent to each Lift landing. The faceplate shall be made of ***stainless steel grade 316. The Stainless steel plate should be at least 2.5 mm thick*** and its mounting arrangement should have two Sunken Screws.....the illumination shall cease. ***The buttons should be permanently illuminated. Illumination Sizes and Finishes should be submitted by the Contractor to “Employer/Employer’s Representative” for review and finalization during detailed design phase.***
42	Part 2: Section VI-B: Technical Specifications: Lifts	5.11	The faceplate of the car position indicator shall be made of scratch-resistant stainless steel grade 304 . Final finish shall be as per the approval of the Employer during design stage /prototype test. The Stainless steel plate should be minimum 3 mm thick and its mounting arrangement should have two sunken screws.This plate.....there is no announcement being done.	The faceplate of the car position indicator shall be made of ***stainless steel grade 316*** .Final finish shall be as per the approval of the Employer during design stage /prototype test. The Stainless steel plate should be ***atleast 2.5 mm*** thick and its mounting arrangement should have two sunken screws. This plate.....there is no announcement being done. This will be reviewed and finalised during the design stage.
43	Part 2: Section VI-B: Technical Specifications: Lifts	5.9.4	**Last Line of the paragraph.** If the doors are prevented from closing by the pressing of hall and/or car buttons or a person in their path for an adjustable pre-set time, the safety devices, except the mechanical door safety edge, shall be rendered inoperative to cause door reversals.	**Last Line of the paragraph.** If the doors are prevented from closing by the pressing of hall and/or car buttons or a person in their path for an adjustable pre-set time, the safety devices shall be rendered inoperative to cause door reversals.
44	Part 2: Section VI-B: Technical Specifications: Lifts	5.17.15	All the safety devices/switches shall be provided with IP 67 level of Ingress Protection	***All the safety devices/switches in the Lift pit shall be provided with IP 67, Hoistway & Shaft safety devices/switches shall be provided with IP 55 and all other remaining safety devices/switches shall be provided with IP 54.*** ***This will be reviewed and finalised during the design stage.***

C4-AES-05-L&E (Addendum-01)				
Sl. No.	**Part/Section**	**Clause No.**	**Original Bid Condition**	**Revised Bid Condition**
45	Part 2: Section VI-B: Technical Specifications: Lifts	5.7.4	Guide rail brackets shall be of hot-dipped galvanized steel.	Guide rail brackets shall be Hot-dip Galvanized**/Spray Galvanized steel.**
46	Part 2: Section VI-B: Technical Specifications: Lifts	5.18.20	Provide necessary travelling cables with 10% spare capacity. FRLS/FRLSZH type Flame and moisture-resistant outer cover which shall not emit toxic fume when affected by fire. Prevent travelling cable from rubbing or chafing against Lift shaft or equipment within Lift shaft. The voltage grade & insulation requirement of the travelling cable should be as per the IS 14665. Separate cables..... acceptance by the Employer/Employer's Representative.	Provide necessary travelling cables with 10% spare capacity. FRLS/FRLSZH type Flame and moisture-resistant outer cover which shall not emit toxic fume when affected by fire. Prevent travelling cable from rubbing or chafing against Lift shaft or equipment within Lift shaft. The voltage grade & insulation requirement of the travelling cable should be as per the IS 14665***/EN 50214*** . Separate cables..... acceptance by the Employer/Employer's Representative.
47	Part 2 Section VIB Techncial Specification-Escalators	6.4.6.10	The chain rollers / wheels shall have durable elastomeric materials bonded to a metal die case hub. The shore hardness of the tyre materials shall be 92º ± 3ºA when cured. The bond shall have sufficient strength to avoid de-tyring under all load conditions.	The chain rollers / wheels shall have durable elastomeric materials bonded to a ***Metal or Poly Urethane die case hub*** . The shore hardness of the tyre materials shall be 92º ± 3ºA when cured. The bond shall have sufficient strength to avoid de-tyring under all load conditions.
48	Part 2 Section VIB General Specification	5.2.6	The Contractor shall be responsible for co-ordinating all aspects of his design and installation including the verification of Combined Services Drawings and SEM Drawings with the designs of the Interfacing Contractors	The Contractor shall be responsible for co-ordinating all aspects of his design and installation including the verification of Combined Services Drawings and SEM Drawings with the designs of the Interfacing Contractors. ***Contractor shall submit Construction Reference Drawings for Lifts and Escalators to Employer/Employer's Representative for NONO. On obtaining NONO, shall submit the same to interfacing contractor/s and co-ordinate for the execution.***
49	Part 2 Section VIB Techncial Specification-Escalators	6.4.4.3	Where necessary, all outer sides of the balustrades and truss shall be provided with reinforced claddings. The gap between Escalators and the sides of Escalator and the adjoining walls / parapet walls shall be provided with decking extensions. The gap between Escalators and the sides of Escalator and the adjoining walls / parapet walls shall be provided with decking extensions. The Contractor shall allow a gap .....notice of no objection by the Employer/Employer's representative.	Where necessary, all outer sides of the balustrades and truss shall be provided with reinforced claddings. The gap between Escalators and the sides of Escalator and the adjoining walls / parapet walls shall be provided with decking extensions.***The gap between Escalators and the sides of Escalator and the adjoining walls / parapet walls/Staircase shall be provided with decking extensions maximum up to 300mm by the Escalator Contractor.*** The Contractor shall allow a gap of approximately 15mm between the decking and the adjacent walls /parapet walls..... All joint lines of interior decking, exterior decking/decking extension shall be aligned and staggered in arrangement in line with the joint line of interior panel. ***Common decking should be provided for parallel escalators.*** The design and the fixing details are subject to the notice of no objection by the Employer/Employer's representative
50	Part 2 Section VIB Techncial Specification-Escalators	6.10.3 (a)	Two sets (one set means for both upper and lower landing of one Escalator) of maintenance barriers shall be provided for stations having less than 8 (eight) Escalators (in one station). Four sets of maintenance barriers shall be provided for stations having more than 7 (seven) Escalators (in one station)	Two sets (one set means for both upper and lower landing of one Escalator) of maintenance barriers shall be provided for stations having less than ***7 (seven)*** Escalators (in one station). Four sets of maintenance barriers shall be provided for stations having more than 7 (seven) Escalators (in one station)
51	Part 2 Section VIB Technical Specification-Escalators	6.4.2.1	Stainless steel comb plates, Corrosion resisting die-casted aluminium alloy comb section..... permit simple replacement in sections. The yellow colour light in the pits shall be provided to demarcate the moving and the non-moving parts of the Escalators. The Escalator Contractor shall provide UPS of suitable capacity with 1 hr back-up to feed power to Comb light, pit light, etc. during main power failure.	"Stainless steel comb plates ***or*** Corrosion resisting die-casted aluminium alloy comb section ..... permit simple replacement in sections. The ***green*** colour light in the pits shall be provided to demarcate the moving and the non-moving parts of the Escalators. The Escalator Contractor shall provide UPS of suitable capacity with 1 hr back-up to feed power to Comb light, pit light, etc. during main power failure".
52	Part 2 Section VIB Techncial Specification-Escalators	6.4.7.16	Minimum two chains or one Duplex chain for the main drive shall be provided for each escalator. Each chain of the main drive shall be capable to run the escalator individually. Where more than two drive motors are used, each drive system shall have minimum of two chains, or one Duplex chain as described above. The drive chain monitoring contacts shall be provided	Minimum two chains or Duplex***/Triplex*** chain for the main drive shall be provided for each escalator. Each chain of the main drive shall be capable to run the escalator individually. Where more than two drive motors are used, each drive system shall have minimum of two chains or as described above. The drive chain monitoring contacts shall be provided.
53	Part 2 Section VIB Techncial Specification-Escalators	6.12	-	**New Item Added** **Condition Based Monitoring (CBM) for Escalators** **Refer Attachment 5 enclosed.**
54	Part 2 Section VIB Techncial Specification-Escalators	6.4.1.2	Truss shall be supported at both ends (and at intermediate support for vertical rises above 5.5m) with resilient supports and bearing plates. The provision of bearing plates…..at 3 locations (Left/Centre/Right) on both landings.	Truss shall be supported at both ends (and at intermediate support for vertical rises above ***5m***) with resilient supports and bearing plates. The provision of bearing plates…..at 3 locations (Left/Centre/Right) on both landings.
55	Part 2 Section VIB Techncial Specification-Escalators	6.4.1.5	The upper constant length will be assumed as 4000mm for vertical rises up to 7.5m, 4500mm for vertical rises above 7.5m to 10m and 4850mm for vertical rises above 10m up to 15m.	The upper constant length will be assumed as ***4500mm for vertical rises up to 7.5m, 4935 mm for vertical rises above 7.5m.***
56	Part 2 Section VIB Techncial Specification-Escalators	6.10.4 (k)	Control switches shall be housed in watertight enclosures - IP67.	**Deleted. However, Refer Clause No. 6.3.17.**
57	Part 2 Section VIB Techncial Specification-Escalators	1.4.1	Terms used are defined in the latest edition of "Safety of Escalators and moving walks: Part1: Construction and Installation" EN 115 & European Machinery Directive (98/38/EC)	Terms used are defined in the latest edition of "Safety of Escalators and moving walks: Part1: Construction and Installation" EN 115 & European Machinery Directive (98/38/EC)/***Machinery Directive 2006/42/EC***
58	Part 2 Section VIB Techncial Specification-Escalators	6.3.16 (a) 6.10.4 (a)	Truss, tension carriage, main drive, floor plate and comb plate supporting structure and backing: Hot-dipped galvanised, minimum thickness 85µm. The truss of Escalator shall be hot dipped galvanized (minimum thickness of 85 micro meter of galvanization to be maintained).	***Truss, Floor plate and Comb plate supporting Structure and backing:- To be Hotdipped Galvanized as per IS 209 and Indian Railway RDSO specification ETI/OHE/13 latest version. Zinc coating shall not be less than 1000 g/m^2 subject to review & acceptance during Design Stage. Tension Carriage and Main Drive may be provided with alternative Anti – corrosion treatment (like 3 layers Painting) subject to review & acceptance during Design Stage.***
59	Section - VI C : Employers Drawings	Employers Drawings	Shaft size for Lift 1 & Lift 2 is mentioned as 1975mm (W) x 2575mm (D)	***Car inside area shall be min. 2.24 Sq. m and shall comply with Clause No. 4.14 of Part-2 Technical Specifications which can be accomodated within the given shaft dimensions. Sizes can be finalised during design stage.***

C4-AES-05-L&E (Addendum-01)				
Sl. No.	**Part/Section**	**Clause No.**	**Original Bid Condition**	**Revised Bid Condition**
60	Part 2 Section VIB Technical Specification- Lifts	5.2.1	Each Lift shall have its own heavy duty driving machine. The method of drive shall be Electric Traction with Gear less IE3 Induction/Permanent Magnet Synchronous Motor (P.M.S.M) having closed loop VVVF Control. (Regenerative feature as optional, at Employer's discretion. Supporting detailed calculation of energy saving viz a viz cost saving shall also be submitted during design stage). a) The System, including ..... of proven design b) The Lifts Sub-systems ..... to be submitted	Each Lift shall have its own heavy duty driving machine. The method of drive shall be Electric Traction with Gear less IE3 Induction/Permanent Magnet Synchronous Motor (P.M.S.M) having closed loop VVVF Control. a) The System, including ..... of proven design. b) The Lifts Sub-systems ..... to be submitted.
61	Part 2 Section VIB Technical Specification- Escalators	4.14.2 (j)	Seismic Zone: Comply with Code requirements for seismic risk zone III, as per IS: 1893-Part 1&2 latest version	Seismic Zone: Comply with Code requirements for seismic risk zone III, as per IS: 1893-Part 1&2 latest version & shall comply with Part-8 Section 5A of NBC 2016 or latest version for Lifts and Escalators.
62	Part 2 Section VIB Technical Specification- Lifts	5.15.2	**Second Line of the paragraph.** The faceplate of the car position indicator shall be made of scratch-resistant stainless steel grade 304 hairline finished. Finish shall be as per the approval of the "Employer/Employer's Representative" during detailed design / prototype test. The Stainless steel plate should be minimum 3 mm thick and its mounting arrangement should have two sunken screws. This plate should be pilfer proof.	**Second Line of the paragraph.** The faceplate of the car position indicator shall be made of ***stainless steel grade 316*** . Finish shall be as per the approval of the "Employer/Employer's Representative" during detailed design / prototype test. The Stainless steel plate should be minimum ***2.5 mm*** thick and its mounting arrangement should have two sunken screws. This plate should be pilfer proof.
63	Part 2 Section VIB Technical Specification- Lifts	5.10.2 (b)	Two vertical rows (where appropriate) of car call buttons for floor designations bearing numerals/ alphabets with integrated tactile push button having Braille code for visually impaired. Braille code on the side of the push button is subject to the acceptance by the "Employer's Representative"	Car call buttons for floor designations bearing numerals/ alphabets with integrated tactile push button having Braille code for visually impaired. Braille code on the side of the push button is subject to the acceptance by the "Employer/Employer's Representative"
64	Part 2 Section VIB Technical Specification- Lifts	4.14.1 (s)	Seismic Zone: Comply with code requirements as per IS: 1893-Part 2 -2002	Seismic Zone: Comply with Code requirements for seismic risk zone III, as per IS: 1893-Part 1&2 latest version & shall comply with Part-8 Section 5A of NBC 2016 or latest version for Lifts and Escalators.
65	Part 2 Section VIB Technical Specification- Lifts	Appendix-C	Mid Landing proposed	Read as "***Emergency Landing***" as per applicable Lift code/standards latest version.
66	Part 2 Section VIB Technical Specification- Escalators	6.3.16 (i)	Refer to clause 6.4.5.1	Read as "***Refer to clause 6.4.4.1".***
67	Part-1, Section - III Evaluation and Qualification Criteria (EQC)	2.4.1	General Experience	General Experience (Revised) **Refer Attachment-08 enclosed.**
68	Part-1, Section - IV Bidding Forms	4.5.1	Price Centre "A1" - Preliminaries and General Requirements	Price Centre "A1" - Preliminaries and General Requirements (Revised) **Refer Attachment-09 enclosed**
69	Part 2 Section VIB Technical Specification- Lifts	4.9.1.3 (g)	The Lifts shall achieve MTTR of 30 minutes	The Lifts shall achieve MTTR of ***60 minutes***
70	Part 2 Section VIB Technical Specification- Lifts	5.23.1	All steel components shall be hot dipped galvanized in accordance with BS 729, with minimum thickness of 85 µm	All steel and structural steel components shall be hot dip galvanized as per IS 209 and Indian Railway RDSO specification ETI/OHE/13 latest version. Zinc coating shall not be less than 1000g/m^2
71	Part 2 Section VIB Technical Specification- Escalators	8.1.1	The design of each component shall achieve the minimum service life given below. The failure rate ..... that corridor. **Escalators Parts** — **Service life(years)** i.Steps — 15 ii.Relays, timers and control gear — 10 iii.Handrail drive system — 15 iv.Step chains and step axles — 15 v.Tension carriage assembly — 15 vi.Main drive assembly — 15 vii.Emergency brake assembly — 15 viii.Step and chain rollers — 15 ix.Handrail — 7 x.Ball or Roller Bearing — 1,10,000 operating hours	The design of each component shall achieve the minimum service life given below. The failure rate ..... that corridor. **Escalators Parts** — **Service life(years)** i.Steps — 15 ii.Relays, timers and control gear — 10 iii.Handrail drive system — 15 iv.Step chains and step axles — 15 v.Tension carriage assembly — 15 vi.Main drive assembly — 15 vii.Emergency brake assembly — 15 viii.Step and chain rollers — 15 ix.Handrail — 7 x.Ball or Roller Bearing — 1,10,000 operating hours **xi.Truss — > 30**

ATTACHMENT-01

ISS & CYBER Security Technical Requirements

Attachment-01

ISS & CYBER Security Technical Requirements

Indicative IS & Cyber security requirements (but not limited to) for entire CMRL phase II systems and is placed as Appendix -19 of this GS document.

Contractor shall comply with given Cyber security requirements as applicable to their respective system.

As a part of Cyber security requirements, Employer/Engineer will appoint/nominate a Concessionaire (CISO & associates) with whom Contractor shall liaise for receiving further guidelines and instruction and necessary compliance.

Contractor shall refer Technical Specification document also for compliance with other additional Cyber security requirement.

ATTACHMENT-02

APPENDIX-19

ISS & CYBER SECURITY TECHNICAL REQUIREMENTS

Attachment-02

CHENNAI METRO RAIL LIMITED

CHENNAI METRO RAIL PROJECT PHASE 2

TENDER No. C4-AES-05-L&E

TABLE OF CONTENTS

CHENNAI METRO RAIL LIMITED

CHENNAI METRO RAIL PROJECT PHASE 2

TENDER No. C4/ASA05

"DESIGN, MANUFACTURE, SUPPLY, INSTALLATION, TESTING & COMMISSIONING OF TELECOMMUNICATION SYSTEM FOR CMRL PHASE II - CORRIDOR 4"

PART - 2

EMPLOYER'S REQUIREMENTS

SECTION VI A

GENERAL SPECIFICATIONS

APPENDIX-19

ISS & CYBER SECURITY TECHNICAL REQUIREMENTS

ISS & CYBER SECURITY TECHNICAL REQUIREMENTS

Table of Contents

List of Tables

List of Figures

1. Introduction

All references in this document to clauses or Appendices of the Agreement are intended and shall be deemed to be references to clauses and Appendices of the Agreement document.

In this document, capitalized words or phrases shall have the meaning ascribed to them in the Agreement (Definitions).

Any capitalized words, terms, phrases, or abbreviations used or explicitly defined in any clause, section, paragraph, or article of this document shall have the meaning set forth therein.

Where such words or phrases are not capitalized, they shall have the meaning consistent with the context.

This document is incorporated into and constitutes and forms an integral and substantive part of the Agreement. Without derogating from the foregoing, this document should be read in conjunction with all Agreement documents.

This document does not describe all obligations or responsibilities of the Concessionaire in respect of the execution of the Chennai Metro Project pursuant to the Agreement. Nothing stated or contained or not stated or not contained in this document shall limit or derogate from any of the Concessionaire's duties, obligations, and responsibilities under and pursuant to the Agreement and Law.

2. Scope and General Provisions

The Systems and Information Technologies (IT) of the Chennai Metro Project collects and processes a variety of digital information, including safety-critical and sensitive information. throughout the Chennai Metro Project, the Concessionaire shall implement measures to protect information and the supporting systems from unauthorized access, modification, destruction, whether accidental or intentional, and to ensure authenticity, integrity, and availability of the information systems.

For the purpose of this document:

Information Technology (IT) assets shall be deemed to include all of the following: information and communication technology systems, including computer systems, Industrial Control Systems (ICS) and SCADA, network and security devices, assets which process, store, transmit or monitor digital information, and all other systems mentioned in this Chapter.

Information Security is a series of means and measures implemented with respect to all Metro systems in order to protect the information processed, stored, and transmitted by the Metro System. In addition, it covers the security of information technology facilities and off-site information storage, computing, telecommunications, and applications related services and connectivity.

Information Security consists of several security services: communications security, data security, software security, operations security, and technological means.

For the purpose of this Chapter and the Information Security requirements, the “Gartner Magic Quadrant” referred to herein pertains to publications from FY2021 and onwards at www.gartner.com “Gartner Magic Quadrant” research notes.

Reference in this Chapter is made to security-related procedures and requirements of CMRL and any other relevant Authority. Notwithstanding any such specific references, the following shall apply:

The Concessionaire is responsible for complying with and implementing all conditions imposed by or pursuant to the procedures and requirements of CMRL or any other Authority.

Such procedures and requirements and/or the conditions for their fulfillment may be amended or updated from time to time, and CMRL, and/or any relevant Authority may, at their discretion, issue or impose any number of additional modified and/or replacement procedures, requirements and/or conditions (including, inter alia, as per the provisions of Sections 6.11 ,6.12 & 6.13 Qualified Personnel) below. The Concessionaire shall comply with any such updates and amendments.

Notwithstanding that security-related risks are not always predictable, and notwithstanding that security-related considerations, means, methods, and/or solutions are constantly developing and evolving, the Concessionaire shall be deemed to have evaluated, assessed, and taken into account all risks and costs associated with complying with its security-related obligations under and pursuant to such procedures and requirements, the Agreement and Law.

The provisions of this Chapter are neither intended nor shall be construed as limiting or derogating from the Concessionaire's obligations to comply with and implement any and all applicable Laws, Permits, and requirements of applicable Authorities, whether in respect of security-related matters or otherwise.

This document establishes the minimum requirements for the Information Security System (ISS) for the Metro System with the goal of protecting the data availability, integrity, and confidentiality of Metro System computing and information systems.

The document also includes Information Security requirements pertaining to other Work Packages covering communication and systems in the Chennai Metro Project. The Concessionaire shall take these into consideration in the design and execution phases.

This document addresses the minimal security considerations and measures in the following areas:

Authentication and identification

Authorization and access control

Network security

Data security

Security architecture

Security administration

Network devices

Server, host and end-point security

Application and database security

Audit and monitoring

System availability and continuity

Physical security

3. Reference Documents and Standards

3.1 Applicable Laws and Standards

The Concessionaire shall design in compliance with all applicable laws and standards, including the standards specified below.

Standard	Description
EN 50159	Railway applications – communication, signalling and processing systems. Safety-related communication in transmission systems
EN50125	Railway applications – environmental conditions for rolling stock and on-board equipment.
FIPS -140	U.S. government computer security standard for the accreditation of cryptographic modules
IEC 62443	Industrial Communication Network – IT Security for Networks and Systems
ISO 27001:2013	Information Technology - Security techniques - information security management systems
NIST SP 800-125	Guide to Security for Full Virtualization Technologies
NIST SP 800-30	Guide for Conducting Risk Assessments
NIST SP 800-53	Recommended Security Controls for Federal Information Systems and Organizations
PCI DSS	Payment Card Industry Data Security Standard
TS 50701	Railway Applications – Cyber Security

The P-SCADA and F-SCADA shall comply with the following Information Security standards:

Standard	Meaning
IEC 62443	Industrial Network and System Security
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security
CEA Guidelines 2021	Central Electric Authority Guidelines (Cyber Security in Power Sector) , 2021
ISO/IEC 15408	Common Criteria Certification Standard
ISO/IEC 17011	General requirements for accreditation bodies accrediting conformity assessment bodies
ISO/IEC 17025	General requirements for the competence of testing and calibration laboratories
ISO/IEC 21827	Systems Security Engineering
SSE-CMM	Capability Maturity Model
ISO/IEC 24748-1	Systems and software engineering — Life cycle management — Part 1: Guidelines for life cycle management.

Standard	Meaning
ISO/ IEC 27019	Information technology — Security techniques — Information Security controls for the energy utility industry
ISO/IEC 61508	Functional Safety of Electrical / Electronic / Programmable Electronic Safety-related Systems
IEC 61850	Communication networks and systems for power utility automation
IEC 62351	Standards for Securing Power System Communications
IS 16335	Power Control Systems – Security Requirements.

4. Acronyms, Abbreviations

In this document, the following abbreviations shall have the meaning ascribed thereto hereunder:

Acronym	Meaning
AAA	Authentication, Authorization and Accounting
ACL	Access Control Lists
OAIT	Administrative & Communication Network
ACS	Access Control System
AD	Active Directory
AES	Advanced Encryption Standard
AFC	Automatic Fare collection
ATS	Automatic Train Supervision
AV	Anti-Virus
BIOS	Basic Input / Output System
C&C	Command and Control
CBN	Communication Backbone Network
CBTC	Communications Based Train Control
CDR	Content Disarm and Reconstruction
CI/CD	Continuous Integration / Continuous Delivery
CSOC	Cyber Security Operation Center
DALC	Data Access Layer Component
DCC	Depot Control Center
DDoS	Distributed Denial of Service (attack)

Acronym	Meaning
DHCP	Dynamic Host Configuration Protocol
DID	Defense-In-Depth
DLP	Data Leak Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DPI	Deep Packet Inspection
DR	Disaster Recovery
DRP	Disaster Recovery Plan
ECMP	Equal-Cost MultiPath
EDR	Endpoint Detection and Response
FIPS	Federal Information Processing Standards
FW	Firewall
HMI	Human Machine Interface
HW	Hardware
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IMS	Incident Management System
IP	Internet Protocol
IPS	Intrusion Protection System
IPSEC	Internet Protocol Security
ISA	International Society for Automation
ISS	Information Security System
LAN	Local Area Network
MAC	Media Access Control
MDM	Mobile Device Management
NAC	Network Access Control
NAT	Network Address Translation
NDAA	National Defense Authorization Act

Acronym	Meaning
NIST	National Institute of Standards and Technology
NMS	Network Management System
NOC	Network Operation Center
OCC	Operation Control Center
OTP	One Time Password
OWASP	Open Web Application Security Project
PAS	Public Announcement System
PBX	Private Branch Exchange
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSIM	Physical Security Information Management
PSTN	Public Switched Telephone Network
PT	Penetration Testing
PTO	Permit to Operate
QoS	Quality of Service
RBAC	Role Based Access Control
RMCS	Radio Mobile Communication System
ROIP	Radio over Internet Protocol
RPF	Reverse Path Forwarding
RSS	Railway Scheduling System
SAM	Security Account Manager (MS Windows)
SCADA	Supervisory Control and Data Acquisition
SCN	Signalling Communication Network
SDLC	Software Development Lifecycle
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SM	Sparse Mode
SMS	Short Message Service

Acronym	Meaning
SOC	Security Operation Center (physical)
SQL	Structured Query Language
SRA	Secure Remote Access
SSH	Secure Shell
SSL	Secure Sockets Layer
SW	Software
TBS	Time Based System
BCC	Backup Control Center
TCMS	Traffic Control Management System
TD	Train Detector
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTR	Trackside Technical Room
UPS	Uninterrupted Power Supply
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WCDS	Wireless Communication Depot System
WWRS	Wideband Wireless Radio System

5. Project IT Infrastructure Overview

The Metro System IT infrastructure shall be implemented based on physically and logically autonomous environments including:

Signaling CBTC (SCN)

- Non Vital Network
- Vital Network

Telecommunication Backbone Network (Operational Communication Network)

Administrative & Communication Network (OAIT)

The administrative systems and applications shall be provided by the Concessionaire. The security solution shall be designed and implemented with all the security means to be ready to absorb the administrative systems, including interfaces to other environments.

As part of the desired functionality and services, some of these core networks shall be expandable and shall provide interconnectivity with external service provider networks and institutions via direct links or dedicated network segments. Implementation decisions for the external connectivity shall follow the security guidelines, as defined in the following security requirements.

6. General Requirements

The Concessionaire shall ensure that the Information and cyber security control measures architecture shall comply with the provisions of this Chapter.

The Concessionaire shall ensure that the information and cyber security concept as detailed in chapter 8.2 is implemented in compliance with all applicable Laws and standards

The security measures shall address the independent and disparate environments in the Chennai Metro Project as described above.

The Concessionaire shall deliver the technical infrastructure necessary to integrate security controls. This infrastructure shall be consistent with the security technologies as defined herein.

The Information Security solution shall focus on enhancing the business practices and procedures that are being utilized by the Metro System and should not be the driving force for the Metro System's business practice and procedures flow.

The Information Security controls and products shall be adapted to meet all other requirements of the Agreement, and as such, shall support the necessary SCADA protocols. The software and hardware components shall be manufactured by companies listed as leaders 1-4 in the Gartner Magic Quadrant.

The proposed security infrastructure shall provide the needed functionality with as little impact as possible upon the Metro System. The solution shall cover all risks presented in the Concessionaire Initial Risk Analysis.

The proposed solution shall have the potential to be scaled in the future, to enable straightforward integration of additional acquired resources into the system. Horizontal and vertical scalability of the solution is required to enable the future expansion of the proposed solution to accommodate a broader range of users.

During implementation, the Concessionaire is required to develop, maintain and update the Information Security policy and procedures.

An Information Security Manager for the Metro System shall be appointed by the Concessionaire. The Information Security Manager shall maintain ongoing contact with CMRL, and shall be responsible, on behalf of the Concessionaire (and without derogating from the Concessionaire’s responsibilities and obligations) for the implementation of the Information Security requirements and for ensuring they are followed. The Information Security Manager shall be approved in advance by CMRL. The CHENNAI Metro Project’s Information Security Manager shall monitor the level of Information Security in accordance with the requirements defined by CMRL. See additional requirements in section 7.2.

Without derogating from the requirements of– Security and Emergency Preparedness Policy, all personnel involved in the Design, Construction (including implementation, installation, Testing and Commissioning) and Maintenance of mission critical systems in the Metro System (such as, for example, [signaling and CBTC, SCADA, Communication & IT systems and Security Systems), shall undergo security clearance and reliability checks in accordance with the procedures of CMRL (as amended or updated from time to time).

Only qualified personnel , following and reliability checks, shall take part in the Design, Construction (including implementation, installations, Testing and Commissioning) and Maintenance of mission critical systems (“Qualified Personnel”).

Qualified Personnel may, from time to time, be required to re-qualify and/or undergo periodic or additional security reliability checks in accordance with the procedures of CMRL (as amended or updated from time to time).

Without derogating from the generality of the provisions of Section [2] (Scope and General Provisions) above or of the foregoing, updates or amendments to the procedures of CMRL may apply, inter alia, to: (i) the definition of “mission critical systems”; and (ii) the level of security clearance required with respect thereof.

According to the instructions of Security and Emergency Preparedness Policy, the Concessionaire shall prepare itself to manage cyber security incidents, including training and mobilizing an Incident Response (IR) team and a negotiation team (in the event of a ransomware incident) that specialize in managing such incidents, and which shall be managed by the CSOC. These teams shall provide on-site and off-site response, depending on the characteristics of the and emergency.

Remote access to the Metro System shall be possible only via VPN secured and authenticated communication.

Anti-malware, anti-spam, anti-spyware, etc. software shall be installed on all computers.

Personal Firewalls shall be installed on Workstations.

Laptop disks shall be encrypted.

All servers and Workstations shall be hardened.

6.1 Equipment Power Supply

Power supply

a. The equipment shall operate on a voltage of 230VAC 50Hz, unless defined otherwise.

b. Equipment that supports redundant power supply shall support power intake from two different power supply sources.

c. Redundant power supplies shall be used as required.

Power supply interruption & UPS (Uninterruptible Power Supply)

a. The proposed ISS, including all related equipment, both in the OCC and at the DCC/BCC, shall be connected to an Uninterruptible Power Supply (UPS) that shall provide backup power to the equipment housed at each site.

b. UPS requirements for all subsystems equipment including ISS equipment is described in Communication Systems .

7. Project Management Arrangements

7.1 Local Contractors and Qualified Personnel

The ISS scope of work, including all its components – planning and design, procurement, integrating, testing, operation and maintenance – shall be fully executed by a local national sub-contractor employing personnel with security certification/s (“Qualified Personnel”), valid during the period of activity associated with the project, as indicated above.

7.2 Concessionaire's Cyber Security Professional Team

Concessionaire personnel dedicated to cyber security. The Concessionaire shall recruit and employ dedicated professional personnel to handle cyber security issues throughout all project phases (planning and design, assimilation, operation and maintenance). The dedicated professional personnel shall include the following:

a. CISO – Chief Information Security Officer, a Concessionaire employee working full-time, with valid security certification/s. The CISO shall provide professional guidance and support to the contractors and sub-contractors acting on the Concessionaire's behalf. He shall be responsible for the following:

   i. Assimilating the Information Security and cyber protection requirements, as detailed in the ISS Requirements document.

   ii. Writing an Information Security master plan, as well as security procedures for the planning, design and establishment phase of the project, and security procedures for the operation and maintenance of the Metro system.

   iii. Leading the Information Security and cyber protection setup throughout all phases – planning and design, procurement, installation, integration, testing, operation and maintenance.

b. Qualifications required of the CISO

   i. The following valid certificates – CISO, CISSP, CISM, CISA, CSSA or equivalent.

   ii. More than 5 (five) years of experience in managing Information Security in National and international projects, including supporting specifically in Information Security and cyber protection aspects in the planning and design, procurement, installation, integration, testing, operation and maintenance phases.

   iii. Extensive knowhow in the protection of IT and OT infrastructures and systems.

   iv. In-depth familiarity with up-to-date technologies and Information Security regulation pertaining to the field of transportation.

c. The CISO shall undergo an interview and shall be appointed pending the approval of CMRL.

Additional personnel dedicated to cyber security. The providers of the following systems and disciplines shall each appoint an Information Security lead:

a. Rolling Stock.

b. Signalling and Train Control.

c. Communication and Data Center.

The areas of responsibility of the above providers' Information Security leads include:

a. Managing the Information Security and cyber protection aspects in the providers' offices, to provide and ensure a safe and secure project work environment.

b. Implementing the guidelines dealing with the providers' areas of responsibility and reporting to the organizational CISO on a regular basis.

c. Managing the design, installation, assimilation and operation of the Information Security System (ISS) components associated with their activity and scope of work.

The qualifications required of the sub-contractors' Information Security leads for the systems mentioned above are:

a. A following valid certificates – CISO, CISSP, CISM, CISA, CSSA or equivalent.

b. More than 3 (three) years of experience in managing Information Security in projects that include IT and OT infrastructures and systems.

The CISO, together with the providers' Information Security leads, shall comprise the Concessionaire's Information Security team throughout all phases of the Chennai Metro Project.

8. General Information Security Requirements

8.1 General Requirements

The Cyber Security Management Plan and cyber security procedures shall be prepared and provided to CMRL for approval during the Development Phase. Without derogating from the generality of the provisions of the Agreement, the Cyber Security Management Plan and cyber security procedures shall comply with CMRL's guidelines.

The proposed system and security architecture shall be designed according to the Concessionaire's Information Security risk assessment and cyber security risk management plan.

The necessary measures to protect the availability, integrity and confidentiality of the data shall be undertaken.

The security controls shall be based on open architecture standards and shall support a distributed computerized environment.

The security controls shall be scalable and capable of being configured to accommodate different levels of security per environment, user, application, or per endpoint basis.

The proposed products for the entire systems (Including IT infrastructure, networking and security, P-SCADA, F-SCADA, VSS, TBS, etc.) shall conform to the requirement specified herein).

As a rule, the installation of any HW / SW manufactured / produced by a blacklisted company / provider, such as in the US government's National Defense Authorization Act (NDAA), or concerning whom there are official intelligence reports suggesting / indicating exploitation of HW / SW manufactured / produced by it for the purpose of penetrating IT infrastructures, will be prohibited.

The security architecture shall provide the capability to track, record and monitor successful and unsuccessful interactions with all Project Systems and subsystems.

The architecture shall examine the issue of segmentation according to the principle of access authorization.

The infrastructure shall incorporate secure data exchange mechanisms and technologies such as cryptography, key management, access control, authentication, and data integrity, where appropriate.

Activities related to Information Security shall be dynamic. The goal is the compartmentalization and control of information distribution to authorized parties only and as needed, while reducing the impact of internal and external security threats on the IT infrastructure.

A Software Development Lifecycle (SDLC) process shall be implemented throughout the Chennai Metro Project as part of the ISS design and integration, including CI/CD processes, in accordance with CMRL's guidelines.

A Data Leak Prevention (DLP) technology, as well as a DLP procedure policy, shall be completed and provided to CMRL for approval.

8.2 Information and Cyber Security Concept -Defense-In-Depth (DID)

The general objective of defense-in-depth (DID) is to ensure that a single failure, whether equipment failure or human failure, at one level of defense, and even combinations of failures at more than one level of defense, would not propagate to subsequent levels. The independence of different levels of defense is a key element in meeting this objective.

Infrastructure shall be based on implementation of the Defense-In-Depth (DID) concept of a hierarchical deployment of different levels of security controls and procedures in order to maintain the effectiveness of the security solution.

The DID concept shall be implemented through design and operation to provide graded protection against a wide variety of security events, incidents and accidents, including human errors within the Metro System and events initiated outside the Metro System.

ISS implementation shall rely on DID hierarchical deployment for all levels of security controls and procedures.

ISS DID design shall pertain to correlation, detection and protection measures to impede the progress of a cyber intruder, while enabling the Metro System CSOC/NOC to detect and respond to the intrusion and/or security breach while reducing and mitigating the consequences of a breach by relevant technologies.

The Concessionaire shall provide an interface between the Chennai Metro CSOC (HN CSOC's SIEM) and the CMRL SIEM-SOC. The Concessionarie shall provide, operate and maintaine a secure communication medium between Chennai Metro's CSOC and the CMRL SIEM-SOC. The communication and solution and interface required the prior approval of TIS and CMRL.

The ISS DID supporting architecture and products shall address security layers, such as data, application, host, network and perimeter.

For each layer, the following shall be addressed as part of the ISS: Network segmentation; Demilitarized Zones (DMZ); Intrusion Detection System (IDS); Intrusion Prevention System (IPS); Virtual Private Network (VPN); Firewalls (hardware/software); AV/Anti-malware software; Authentication and password security; Encryption; Sandboxing; Hashing passwords; Timed access control; Logging and auditing; Multi-factor authentication; Vulnerability scanners; Physical security (VSS), Central control (NOC, CSOC, SIEM); Audits and logs, Policies; cyber security procedures, including change management.

8.3 Data Leak Prevention (DLP)

DLP technology shall be examined based on the criticality level of the information and data that reside in each of the networks.

The ISS shall implement and deploy strong DLP technology products.

DLP shall pertain to the CBN (data-in-motion) analysis of data traffic, to detect sensitive data sent in violation of Information Security policies. DLP shall be centralized, with distributed agents.

Endpoint (data-in-use) agents or clients shall run on internal end-user Workstations and DC servers. End point shall be used to control information flow between groups or types of users.

DLP shall include data identification techniques, to identify confidential or sensitive structured data in fixed fields within a file or unstructured data, to support content analysis, and contextual analysis

The DLP shall pertain to retention and archived data-in-use and data-in-motion.

8.4 Building Blocks of the Information Security System (ISS)

Prevention – execute all applicable measures to prevent the Metro System's security risk.

Detection – detect and identify in real time unauthorized and illegal activities in the Information Systems.

Response and mitigate – response and mitigate security events.

Audit – execute an accurate and detailed audit on all Information Systems activities.

8.5 Information Security and Supply Chain Risk Management Requirements

8.5.1 General

a. The Concessionaire shall comply with the Information Security requirements of CMRL, which obligate it to implement several actions, as detailed below.

b. The Concessionaire shall submit official documents confirming compliance with Information Security requirements, as defined by CMRL.

8.5.2 Supply chain risk assessment and risk management plan

The Concessionaire shall implement a risk management plan for the critical systems supply chain , as defined in this chapter, with the following outputs:

a. A risk assessment for the supply chain shall be conducted for the entire Chennai Metro System and for the following critical systems - ISS, Communication and IT Systems, P-SCADA, F-SCADA, signaling and CBTC and security systems related equipment and systems.

b. A security management plan for the critical systems supply chain, with specific activities and control measures, shall be completed and submitted to CMRL for approval.

8.5.3 Information Security requirements for design outputs

The requirements listed below shall be complied throughout the Chennai Metro Project.

a. All sensitive digital information (any information that is protected against unwarranted disclosure, such as IP schema, low level designs) shall be encrypted.

b. Sensitive information shall be stored in encrypted and compartmentalized folders, accessed only by users with access authorizations.

c. Remote access shall be allowed via VPN secured communication only.

d. Anti-malware, EDR, anti-spam, anti-spyware, etc. software shall be installed on all computers.

e. Personal firewalls shall be installed on personal computers.

f. Laptop disks shall be encrypted.

g. The level of Information Security shall be monitored in accordance with the requirements defined by CMRL.

8.5.4 Information Security for sensitive technical documents

a. The Concessionaire shall fully comply with CMRL procedures for securing and storing digital files.

b. Information Security arrangements pertaining to servers used for storing files shall be subject to CMRL's approval, and shall be monitored.

c. Access to the server shall be based on access authorizations, and server folders shall be encrypted in accordance with the documents' security classification.

d. Sensitive technical documents shall comply with a sensitive Information Security procedure defined by CMRL, that includes access authorizations to folders, password protection and encryption. The printing of these documents and the dissemination of hard copies shall require documenting the recipients and storage in a physically protected location (room with a burglar alarm, a security cabinet or safe).

8.5.5 Procurement of systems' critical elements

a. The procurement procedure of critical system elements shall follow the CMRL guidelines and shall be subject to CMRL's approval.

b. The critical elements (for example, the communication system's software and hardware) shall be purchased from approved providers see clauses 8.5.6. and 8.5.8 below.

c. The procurement of critical elements, as well their storage, transport to the site and installation shall be monitored.

8.5.6 Installation, integration, testing and handover of systems

a. The Concessionaire shall fully comply with CMRL's and its Information Security requirements during the design, installation, integration, testing and handover of the systems, as well as throughout the Term of the Agreement.

b. The procedures shall be develope, implemented and maintained by the Concessionaire.

c. Tests shall be executed in accordance with CMRL's and its Information Security procedures, including access control and hardening.

8.5.7 Concessionaire's Requirements by Systems and Activities

a. The contractor shall comply with cyber security policy /guidelines for the web-based software applications and its infrastructure to reduce the risk of cyber-attacks and protect against the unauthorised access to the systems, networks, and technologies as per the latest CEA (Cyber Security in Power Sector) Guidelines 2021 issued by Government of India (Comments received from Lift & Escalator).

b. The Concessionaire shall be responsible for each project phase according the matrix in table 1.

c. With respect to all of the following (ISS, Communication and IT Systems, P-SCADA, F-SCADA, signaling and CBTC and Security Systems related equipment and systems):

i. Only generic hardware and software manufactured by manufactures listed as “Leaders 1 to 4” in the “Gartner Magic Quadrant” shall be used.

ii. If a specific hardware or software component is not listed in the “Gartner Magic Quadrant”, three alternative manufactures shall be submitted for the approval of CMRL.

d. In order to ensure a secure supply chain, the Concessionaire shall contract with the local suppliers/branches of the HW and SW components approved by CMRL, and guarantee that the HW and SW components are supplied in India and fully comply with CMRL’s Information Security requirements and CMRL secured supply chain requirments.

e. CMRL reserve the right to reject a certain HW/SW component. The Concessionaire shall be required to replace a rejected component.

It is hereby clarified that such rejection may be due to the HW/SW characteristics and/or manufacturer / developer / provider, if suspected of non-compliance with Information Security requirements, or it is being suspected of Information Security breaches or illicit activities. For this purpose, CMRL may rely on third party information such as the US National Defense Authorization Act (NDAA), or intelligence reports by any international or local governmental agency.

f. Qualified Personnel

i. Only personnel employed by the Consessionaire or by any of its contractors and/or sub-contractors, who have passed the security clearance checks, shall be considered Qualified Personnel. Only Qualified Personnel shall be permitted to take part in the design, installation, integration, configuration and maintenance of the Critical Systems of the Chennai Metro System.

ii. Qualified Personnel may, from time to time, be required to re-qualify and/or undergo periodic confirmations of security clearance or additional security clearance checks in accordance with the procedures of CMRL (as amended or updated from time to time). Please refer also to sections 6.11, 6.12 and 6.13.

8.5.8 Systems Requirements

Table 1: Equipment and Qualified Personnel Requirements for Mission Critical Systems

Sub-System	Equipment and System Related Requirements	Personnel Related Requirements	Restricted Access / Additional Requirements
ISS	The provisions of Sections 8.5.6 shall apply.	The provisions of Section 8.5.7 f. above (Qualified Personnel) shall apply with respect to all personnel involved in the design, construction, testing, commissioning, operation and maintenance.	Only Qualified Personnel on behalf of the Concessionaire shall be provided with access to the ISS for purposes of performing all obligations pursuant to the Agreement with respect thereto.
Communication Backbone Network (CBN)	The provisions of Sections 8.5.6. shall apply.	The provisions of Section 8.5.7 f. above (Qualified Personnel) shall apply with respect to all personnel involved in the design, construction, testing, commissioning, operation and maintenance.	Only Qualified Personnel operating on behalf of the Concessionaire shall be permitted access to the CBN for purposes of performing all obligations pursuant to the Agreement with respect thereto.
Control Centers & Data Center Systems, include the Staging Environment	The provisions of Sections 8.5.6. shall apply.	The provisions of Section 8.5.7 f. above (Qualified Personnel) shall apply with respect to all personnel involved in the design, construction, testing, commissioning, operation and maintenance.	Only Qualified Personnel operating on behalf of the Concessionaire shall be permitted access to the Control Center and Data Center Systems for purposes of performing all obligations pursuant to the Agreement with respect thereto.
P-SCADA	a. The provisions of Sections 8.5.6. shall apply; and b. The Concessionaire shall demonstrate that, as at the date of issuance of Notice to	The provisions of Section 8.5.7 f. above (Qualified Personnel) shall apply with respect to all personnel involved in the design, construction, testing,	Only Qualified Personnel operating on behalf of the Concessionaire shall be permitted access to the P-SCADA for purposes of performing all obligations pursuant to

Sub-System	Equipment and System Related Requirements	Personnel Related Requirements	Restricted Access / Additional Requirements
	Proceeds, [each of] the HMI and the PLCs supplied are installed and in operational use in not less than three (3) Critical Infrastructure Installations in India	commissioning, operation and maintenance.	the Agreement with respect thereto.
F-SCADA	a. The provisions of Sections 8.5.6 shall apply.; and b. The Concessionaire shall demonstrate that, as at the date of issuance of Notice to Proceeds, [each of] the HMI and the PLCs supplied are installed and in operational use in not less than three (3) Critical Infrastructure Installations in India	The provisions of Section 8.5.7 f. above (Qualified Personnel) shall apply with respect to all personnel involved in the design, construction, testing, commissioning, operation and maintenance.	Only Qualified Personnel operating on behalf of the Concessionaire shall be permitted access to the F-SCADA for purposes of performing all obligations pursuant to the Agreement with respect thereto.
signaling and CBTC	a. The provisions of Sections 8.5.6. shall apply, with respect to all signaling and CBTC equipment, HW & SW components; and b. The Concessionaire shall demonstrate that, as at the date of issuance of Notice to Proceeds, signaling and CBTC equipment, sub-system and SW supplied are installed and are in operational use, in	The provisions of Section 8.5.7 f. above (Qualified Personnel) shall apply with respect to all personnel involved in the design, construction, testing, commissioning, operation and maintenance.	Only Qualified Personnel operating on behalf of the Concessionaire shall be permitted access to the signaling and CBTC for purposes of performing all obligations pursuant to the Agreement with respect thereto.

Sub-System	Equipment and System Related Requirements	Personnel Related Requirements	Restricted Access / Additional Requirements
	not less than three (3) Metro, Tram-Train, Metro, Rail or Inter-City Rail Projects, with at least 12km and 5 stations in India.		
Security Systems	a. The provisions of Sections 8.5.6 shall apply, with respect to all security systems equipment (edge devices), HW & SW components; and	The provisions of Section 8.5.7 f. above (Qualified Personnel) shall apply with respect to all personnel involved in the design, construction, testing, commissioning, operation and maintenance.	Only Qualified Personnel operating on behalf of the Concessionaire shall be permitted access to the Security Systems for purposes of performing all obligations pursuant to the Agreement with respect thereto.

For purposes of the foregoing requirements:

(1) A “Critical Infrastructure Installation” shall mean a large-scale critical infrastructure project in a India, such as a power generation facility, a port, Metro system or an airport.

(2) “Metro or LRT Project” shall mean a light rail, Metro or commuter rail-based mass transit system in a India providing transportation services to the public.

Reporting

a. The Concessionaire shall comply with the Information Security incident reporting procedures and incident escalation reporting procedures defined by CMRL (as may be amended from time to time), including attempts to penetrate the system, damage caused to components, theft and attempted theft of components that are intended for installation in the Metro System’s critical systems.

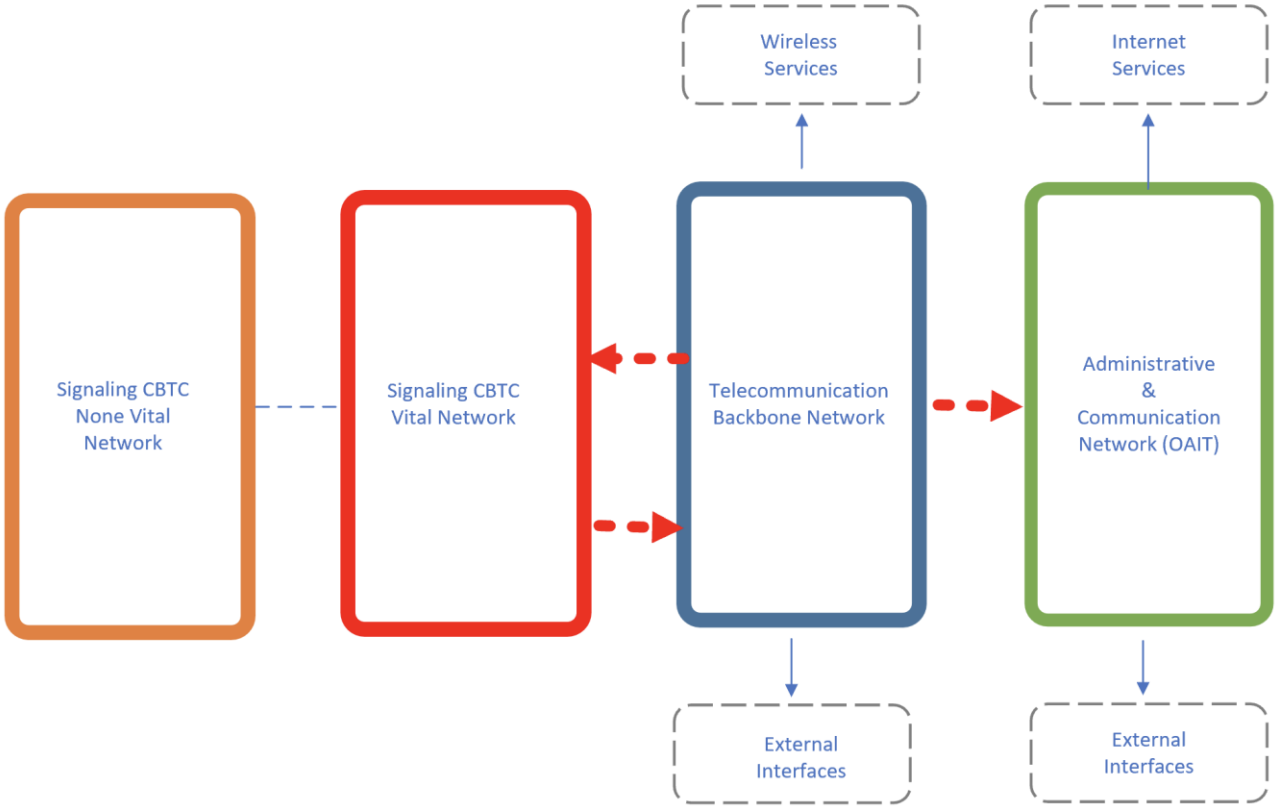
b. The Concessionaire shall implement monitoring and control procedures covering work processes, Design, Installation, Testing and Maintenance of the Metro System’s critical systems, as defined and coordinated with CMRL.

Information records and as-made documents

The Concessionaire shall safeguard electronic records, documents and as-made documents in accordance with CMRL guidelines.

9. Information Security Threats and Impacts

Error! Reference source not found. is an overview of the Metro System's logical a rchitecture and information flow:



1. **Figure 1: Logical Architecture and Information Flow (Conceptual)**

9.1 Risk Assessment

The Risk Assessment of the system's security environment shall be conducted by the Concessionaire as described in section 14.

The Risk Assessment shall be used as the baseline for the system's security design.

9.2 Potential Risk Types

The following non-exhaustive list describes types of security threats related to the Metro System identified during the Initial Risk Analysis:

Impact on the public safety & human lives

Destruction or loss of critical services

Interruption of access to critical services, information or applications

Disclosure or viewing of critical or sensitive information

Modification of critical or sensitive information

Threat prevention and management shall pertain to all known threats at the time of delivery such as the following: Access rate control; Authentication bypass; ARP poisoning; Broken access control; Brute force login; Buffer overflows; Cross site scripting; Cross site request; Denial of Service (DoS); Data Loss Prevention (DLP); Distributed Denial of Service (DDoS); Directory traversal; DHCP spoofing; DNS poisoning; Forms tampering; Hidden field manipulation; Session hijacking; SQL

injection; Site reconnaissance; Schema poisoning; XML parameter tampering; WSDL scanning.

9.3 Attack Vectors

Threat sources shall be considered including:

Terrorists

Internal attackers

Disgruntled staff

Hackers

Criminals

Foreign intelligence services

Organized crime

Protesters and activists (e.g., environmental, political, animal rights)

9.4 Impacts

Safety, health and environmental event or damage to infrastructure: An event that results in harm to individuals, the environment or damage to the infrastructure.

Forced controlled shutdown of operation: An event that results in the emergency shutdown system being automatically invoked with no human intervention, for example, when the view of all or some of the production processes is lost.

Elected controlled shutdown of operations: An event that results in the site electing to shut down its operation, for example, when view of all or some of the production processes is lost.

Reduction in operating efficiency: An event that would result in the system continuing its operation in a less efficient or profitable manner or result in reduced production. For example, operational delays in services provided, or severe environmental change which impacts and limits the ability to use the service.

Loss of business continuity.

Loss of reputation.

10. Security Services and Infrastructure

Security Services shall be implemented as part of the Metro System. For detailed security requirements related to individual core networks, refer to Chapter 11

10.1 Authentication

The system shall prevent simultaneous logins of a single user.

Users shall be automatically logged off after being idle for 15 (fifteen) minutes.

PKI-based (strong authentication) shall be implemented based on the environment addressed. For the different core network solutions, some of the following methods shall be used: OTP, token, PKI certificate, smartcard, biometric, machine certificates.

The System shall detect the number of consecutive unsuccessful authentication attempts and ignore any authentication attempts when the maximum number of authentication attempts defined by the administrator is reached, i.e., the user account shall be blocked.

Authentication attempts shall only be resumed after the administrator explicitly lifts the restriction, or after a predefined timeout.

A password policy that enforces, as a minimum, strength and complexity of passwords, as well as expiration time, shall be implemented for all systems.

Passwords should be changed frequently. Password history shall be used.

User/service authentication shall be based on individual accounts only. No shared accounts are allowed.

User authentication information shall not be exposed on any output.

No clear text login shall be permitted to any system. The login information shall be cryptographically protected on the network/communications level.

10.2 Identification

User identification and authentication shall take place at the network, device, application, and/or device/software level. A user shall be restricted from establishing a secure data exchange without first being identified and authenticated by at least two authentication factors.

The identification service shall be based on a managed directory implemented separately in each one of the System's independent networks.

User groups shall be defined based on administrative units, roles and their functions, with a view to institutionalizing control of access to information.

No default, guest/anonymous, or temporary accounts shall be permitted to any system.

10.3 Authorization and Access Control

Security Architecture

a. Multi-layered and zone-based network architecture meeting updated industry standards shall be adopted to ensure secure and strong segregation between various environments.

b. The various core networks shall be separated. The signaling environment shall be physicaly separated and communicate with the operational environment (TCN) through a guaranteed one-way traffic mechanism. Logical segmentation for each network shall segregate the internal networks.

c. The operational environment (TCN) shall be physicaly separated and communicate with the signaling environment through a guaranteed one-way traffic mechanism.

d. Network segmentation within the various core networks shall be implemented based on the data flow, as will be described in the Concessionaire's Initial risk analysis. The segmentation shall be based on firewalls between the network segments.

e. Further to the network segmentation within the core networks, VLANs, Private VLANs and ACLs shall be implemented for the individual operational services. For example, Directory services shall be in a VLAN, separated and filtered from the DLP services.

f. Separation of development, test and production environments is required. Data transfer between environments shall be done in a controlled manner As per IEC 62443- 4-1.

g. Internet access from/to signalling and operational communication networks shall not be permitted. Any access to the Internet shall be achieved only from the OAIT and through terminal based computing (e.g., Citrix).

h. Every wireless access network incorporated into the system's infrastructure shall be completely separated from all the core networks and from any other wireless network.

i. The separation between the wireless and the core networks shall be obtained on all the levels of system's and include at least a physical separation, Firewall inspection, Dedicated cryptography and VPN tunneling – on the network transport level, communication inspection on the application level. The security measures and architecture of the wireless access networks shall be specifically approved by the CMRL.

j. Privileged user access shall be managed with Privileged access management technology.

k. The Concessionaire shall authorize, control and monitor access privileges to system and information resources to the following entities:

    i. Users (all entities with access to system resources).

    ii. Operations personnel.

    iii. Non-interactive processes.

    iv. Maintenance and support personnel.

    v. Supervisors.

    vi. Systems analysis and programming personnel.

l. The access control mechanism shall be flexible and capable of managing issues such as delegation of rights and changes in roles.

m. Role-Based Access Control (RBAC) shall be implemented based on the type of information accessed and in accordance with the user groups defined.

n. The information system shall employ the concept of least privilege, allowing only authorized accesses for users, and processes or services acting on behalf of users, which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

o. User privileges shall be restricted by:

    i. Controlling user read, write, create, delete and execute capabilities.

    ii. Implementing access control lists.

    iii. Implementing capability lists.

    iv. Controlling hierarchical authorization, such as CMRL, group, system and everything else.

p. All successful logons and any failed logon attempts shall be logged.

q. Network Access Control (NAC) shall be based on IEEE 802.1x or equivalent and shall be implemented for all devices connecting to the system resources and supporting the relevant security protocols. Devices not supporting secure network access technologies should be connected to a separate network segment (physical or virtual [VLAN]), and their access to the network should be protected by a standard network-level security mechanism (such as MAC security), or a dedicated NAC system.

r. Inactivity session timeouts shall be implemented for all applicable systems. Automatic termination of expired sessions and re-authentication of interactive users after a predefined period of inactivity shall be enforced.

s. The Information System shall limit the concurrent sessions for each System account.

Remote Access

a. Remote connection shall allow the systems providers (controllers, software components) to conduct diagnostics and software updates in the Production environment in cases where the Concessionaire, via the various maintainers, did not succeed to complete local maintenance work and/or update software via a local entity in the Staging environment.

b. A cryptography mechanism shall be used to protect the confidentiality and integrity of remote access to information system (e.g., VPN).

c. The Information System shall route all remote access through a limited number of managed access control points.

d. Remote access shall be restricted to specific users and at specific times.

e. The execution of privileged commands on mission critical systems and/or access to security-relevant information, via remote access, shall be authorized only for specific operational needs.

f. In case access is needed by external national authorities (e.g., Police), it shall be based on network extension over a private encrypted secure channel (e.g., dark fiber), and performed from a managed and/or authorized and authenticated client.

g. Remote access methods to SCN and telecommunication backbone network core networks shall be implemented according to CMRL guidelines, and approved by CMRL.

h. The need for remote connection to the operational network shall be evaluated, and a structured process to achieve this shall be proposed.

i. A system supporting the Secure Remote Access (SRA) and the recording of the remote access activity, as well as encryption and timing of the channel opening, shall be provided.

j. Remote access to applications and/or services, performed by mobile endpoints through wireless (Wi-Fi and/or Cellular) network shall be performed from security-hardened endpoints only, against a dedicated network segment.

10.4 Network Security

Proactive network protection shall be implemented based on multiple components/technologies, as follows:

Next Generation Firewall – Firewall devices capable of traffic stateful inspection and certified for Evaluation Assurance Level +2 shall be implemented. The Firewalls shall support traffic separation at interface level, through IEEE 802.1Q VLAN, for logical network partitioning, policy and management separation.

An industrial Firewall that supports the required protocols and performs DPI (Deep Packet Inspection) shall be defined. The Firewall shall also support segmentation, which shall be defined in accordance with the risk assessment and topology analysis.

An Intrusion Prevention System (IPS) and an Intrusion Detection System (IDS) (internally) shall be deployed both externally and internally to the firewall technology

implemented , protecting the network environments. The proposed IPS/IDS systems shall support signature-based, anomaly-based and stateful protocol analysis.

Network Application Firewall – Malicious code protection based on network application firewalling (e.g., content filtering technologies, application gateway firewalls) shall be implemented at the relevant interfaces as described in the following Reference Architecture and information flow Diagram.

End-to-end communication security shall be implemented based on common practice secure protocols such as SSH, IPSec, SSL/TLS.

Access control lists shall be implemented on all network and security devices.

Network client authentication – Network client authentication shall be implemented using common standards such as IEEE 802.1x in the various network segments.

NAC – NAC or equivalent system shall be implemented on every network in the CBN. NAC shall ensure that only the required and approved network connections are allowed. In addition, updated industry standard protocols, encryption mechanisms, mutual authentication and credential protection shall be used.

VoIP Security – the proposed VoIP security solution shall follow industry best practices for VoIP security.

VoIP Systems – the VoIP systems (including RoIP gateways and network extension units) shall have the voice and signalling data logically segregated from the data traffic. VoIP-ready Firewalls shall be employed to secure the proposed VoIP systems.

Public Switched Telephone Network (PSTN) Security – PSTN security shall be based on implementation of dedicated IP PBXs for internal and external voice communications. Voice firewalls shall be employed to secure the proposed IP PBX systems. Telephony security shall also prevent external fraud by unauthorized parties by securing and monitoring the telephony system. Interfaces to external IP PBXs shall be via dedicated Firewalls and VoIP gateways.

Virtualization security practices, if such technology is used, shall follow industry best practices. In addition, a security hardening of the virtualization environment shall be performed according to the virtualization software vendor recommendations.

A virtualization technology solution shall be implemented per each core networks only.

Automatic Clock Synchronization – automatic clock synchronization for computers, networks, security and telecommunication systems shall be secured and shall work through a time Firewall or equivalent in order to mitigate any blocking, jamming, spoofing or any other malicious attack.

Automatic clock synchronization shall comply with Time Based System. All security events shall be synchronized with the TBS. The TBS equipment shall comply with CMRL guidelines.

Updates – the latest version of the operating system/firmware for all security devices shall be used.

A structured Testing environment for updates is required.

10.5 Firewalls

Firewalls shall comply with the following:

Integrated threat intelligence adaptive threat protection against command and control (C&C)-related botnets and policy enforcement based on GeoIP.

Carrier-class routing features of IPv4/IPv6, OSPF, BGP, and multicast.

Firewall Services shall follow industry best practices

Network Address Translation (NAT) shall follow industry best practices.

VPN Capabilities shall follow industry best practices:

a. Threat defense and intelligence services shall provide: Spotlight secure threat intelligence and protection from botnets (command and control); Adaptive enforcement based on GeoIP; Threat prevention to detect and block zero-day attacks; Routing and dynamic routing protocols; Multicast; Encapsulation; Virtual routers; Policy-based routing; Source-based routing; Equal-Cost MultiPath (ECMP); Firewall Quality of Service (QoS); Marking, policing, shaping, classification and scheduling; Guaranteed and maximum bandwidth control; Ingress traffic policing; Virtual channels.

b. Firewall devices switching & network services shall follow industry best practices.

10.6 Data Security

The information system shall protect the integrity and confidentiality of transmitted information at the application level. Mechanisms used to ensure data integrity shall be based on message authentication, hash-functions, and digital signatures.

Industry-recognized cryptographic protocols shall be implemented for message integrity, where applicable, to detect information changes during transmission.

Updated industry-standard cryptographic mechanisms on the applicable data shall be deployed to prevent unauthorized disclosure of information during transmission.

Protection mechanisms detecting and eradicating malicious code (such as viruses, worms, Trojan horses) shall be implemented at information system entry and exit points.

Relevant Protection mechanisms detecting and eradicating malicious code (such as viruses, worms, Trojan horses) shall be implemented at Workstations, servers, or mobile computing devices connected to the network.

The SCN environment – where proactive protection mechanisms can impair system's real-time performance, minimal-impact protection techniques (such as applications and services whitelisting and signing, and monitored and recorded sessions) shall be implemented.

A CMRL approved secure mediation measure (CDR) for controlled mediation and transfer of information from non-trusted sources, such as removable media, to the core networks shall be implemented (E.g. Sasa Software, Opswat, Votiro etc). The mediation process shall follow industry best practices.

10.7 Security Administration

Security policy and procedures

Written IT security policy and procedures shall be developed, issued and submitted to CMRL for approval.

Classification and designation of sensitive information and assets

a. A classification and designation guide that contains procedures for classification, declassification, designation and downgrading of IT information and assets shall be developed. The classification and designation guide shall specifically address all types of information processed in the IT environment.

b. IT assets shall be classified and designated according to their importance, integrity, availability and value.

Separation of duties

a. To the extent possible, it shall be ensured that responsibilities are separated in such a way that no individual has complete control over related critical IT & OT operations.

b. The following duties should be separated:

   i. Operations

   ii. System administration

   iii. Network administration

   iv. Database administration

   v. Application programming/development

   vi. Testing

   vii. Security management

   viii. Production

c. For each of the core networks, management of IT assets shall utilize a solid privilege separation security perception. IT assets shall be concentrated in dedicated, separate based on their function, for example IT resources, back-office, etc.

d. Centralized management for servers and network devices shall be implemented separately in each of the autonomous networks, based on industry recognized NMS (e.g., HP Open View, Cisco Works) and centralized monitoring system that will collect the alerts from the entire NMS system through a diode, to build integrated visibility.

e. Standard Authentication, Authorization and Accounting (AAA) methodology shall be implemented.

f. Network security management – In SCN and telecommunication backbone network core network management shall not be permitted via the Internet, VPN or any third-party network.

g. Cryptographic keys for required cryptography employed within the information system shall be established and managed. Industry best practices key management shall be followed, using full standard PKI.

h. All security devices that contain sensitive cryptographic keys shall not be managed remotely.

10.8 Network Devices

All network devices shall be configured and hardened according to known best practices and guidelines. The exact list of guideline and hardening procedures documents shall be defined and provided to CMRL for approval.

It is required that the latest stable version of the operating system for all network devices is used.

The proposed firmware shall support and follow updated protocols, best practices and industry standards.

All routers/switches shall support and follow updated protocols, best practices and industry standards.

10.9 Server, Host and End-point Security

Each server and workstation shall be configured and hardened according to known best practices and guidelines. The exact list of guideline and hardening procedures documents shall be defined and provided to CMRL for approval. The security capabilities of the operating systems shall be optimally leveraged and configured. Monitoring capabilities shall be implemented on each network, including the SCN, telecommunication backbone network, OAIT, SCADA, TCMS and Rolling Stock On-board equipment as well.

ISS shall incorporate EDR technology (Endpoint Detection and Response) and EPP capabilities, including host Firewall, device control configuration management, disk encryption and Host based IPS, to meet the need for continuous monitoring of and response to advanced threats.

The Concessionaire shall add a capability to remove 'suspected as compromised' mobile devices from the network, manually and automatically (with an override option).

Workstations used for processing and storing sensitive information (i.e. signalling information or any information that will be defined as critical by CMRL) shall be protected with additional control measures, such as containers, MDM or equivalent.

Workstations used for processing and storing critical operational information shall have at least the following security measures implemented: TPM or SAM for secure key storage and operation; Machine BIOS setting shall be protected by password.

Strong malware protection (against zero-day attacks), including: Personal Firewall; Host based IDS/IPS, anti-virus (Endpoint protection & Endpoint detection and response) package.

A device control solution shall be implemented, including applying customized security policies over all physical, wireless and storage interfaces (e.g., USB, modem, Wi-Fi, Bluetooth, and external hard drives).

Mobile computing device security

a. The Metro System's mobile computing devices that contain or have access to the operator information or IT applications shall be protected in accordance with Operator Information Security Policy and Standards. Mobile computing devices shall utilize Operator's approved encryption tools.

b. All mobile computing devices that contain or have access to Metro System Information or IT applications shall have:

    i. Automatic log-off mechanism

    ii. Process to prevent unauthorized viewing of user IDs or passwords

    iii. Safeguards based on the information's classification.

c. The communication connections shall be defined as a private line for predefined use only. The line shall be used to connect the edge equipment (smartphone or tablet) to the system from point to point, without additional connections.

d. Edge devices (smart phone/tablet) shall be hardened and shall ensure the developed application supports the hardening.

e. The devices shall allow the usage of specific applications while blocking Internet surfing, connecting to other public networks, downloading applications and any other use that presents a potential Information Security risk.

f. The option of connecting to Bluetooth and public Wi-Fi networks shall be blocked.

g. The communication channel shall be encrypted via high grade encryptions, such as AES 256.

h. An AAA mechanism shall be defined for access purposes, user identification and authentication.

i. It shall not be possible to insert devices such as disks-on-key into the edge equipment.

j. Preventive CSOC and NOC monitoring operations shall be defined in order to identify attempts to penetrate the system by unauthorized and potentially hostile elements, including the injection of malware.

k. The system shall have autonomous monitoring capability, with alerts sent to the CSOC system in the event that penetration into the system, viruses or malware are detected.

10.10 Application Security

Implemented Services and Applications shall follow industry best practices for secure development:

a. Applications, databases and services shall not run with full operating system privileges and shall be granted the minimum required privileges. Databases shall not be granted admin privileges.

b. The AFC System shall comply with the following high-level security standards as per NCMC norms (CDAC Specification),

c. REST API (HTTPS communication) shall be used for Web Service creation. It supports all modern browsers and mobile applications.

d. File transfers shall take place using secure application protocols like SFTP, HTTPS or TCP/IP with SSL.

e. Applications providing web interfaces shall comply with current OWASP secure web development guidelines.

f. Applications shall never connect to a database using the database administrator account or an account with system or management privileges.

g. Generally accepted principles for secure coding (SDLC) shall be implemented for all applications development.

h. Mobile code – process for authorization, monitoring, and control of the use of mobile code within the information system shall be established.

i. Applications shall utilize prepared SQL statements and/or stored procedures to minimize the risk of SQL injection.

j. All access to the database services shall be implemented using a dedicated Data Access Layer Component (DALC).

k. Applications shall support updated encryption protocols, with 256-bit minimum, for all communications interfaces.

l. The application shall validate all provided inputs and shall not trust submitted or presented data.

m. The application or a security solution above it shall have proper and secure session management to protect the sessions from unauthorized access, modification or hijacking.

n. Standard cryptographic APIs shall be used for cryptographic processing, if applicable (i.e., Bsafe, OpenSSL).

Monitoring

a. A process of monitoring the identification, authentication, authorization and access control, and administration of information infrastructure security shall be implemented to determine if proper security has been established and maintained. All security events shall be managed at a CSOC that shall be installed and operated at the OCC/BCC NOC.

b. The monitoring platform shall include the possibilty for a wide range of queries and analysis capabilities for threat hunting operations and incident investigation.

c. The Information System shall be capable of generating audit information for at least the following security-related events:

    i. Job or process status (entry, initiation, completion, deletion, restart, and abort)
    ii. File, volume, and database accesses where applicable (open, close, create, delete, rename)
    iii. Communications devices connect, disconnect and re-configuration
    iv. Network status messages
    v. User log-on and log-off attempts (including failed attempts and session timeouts)
    vi. System operator commands and responses
    vii. Any actions performed with administrative privileges
    viii. System and subsystem status messages (start-up, shutdown, abort)
    ix. System-generated messages or requests regarding configuration changes
    x. Changes to system logging facility status (start, stop, alter, print, dump, delete, rename and overflow)
    xi. Changes to access control information
    xii. Changes to lists of authorized users
    xiii. Detected security incidents
    xiv. Use of privileged or powerful software
    xv. Unauthorized network scanning such as port scans

d. For each auditable event, at least the following information shall be generated:

    i. Nature and type of incident
    ii. Date and time
    iii. User identification
    iv. Device identification (IP/MAC address, host name)
    v. Job or process identification
    vi. Identification of resource accessed
    vii. Mode of access
    viii. Configuration details
    ix. Details of the performed activity/action (e.g., change password, update permissions)

The system shall maintain the confidentiality of authentication credentials (e.g., passwords) by excluding or masking them in the audit log.

Security event logs shall be generated and kept for each device and system and shall be sent to Security Information and Event Management (SIEM) for further analysis, correlation, and evaluation in order to identify and respond to suspicious activity. The event logs shall be kept for a minimal period of 1 (one) year. The proposed SIEM

system shall support exporting the SIEM event logs to an external/detachable storage device.

The protection of security log information from unauthorized access, modification, and deletion shall be ensured.

A proper audit record storage capacity and configure auditing shall be allocated to reduce the likelihood of such capacity being exceeded.

Audit records shall be retained for a minimal period of 1 (one) year, to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

SIEM platform shall be implemented for centrally collecting, analyzing and correlating generated audit information. The correlation engine shall be capable of generating real time alerts (SMS, email) and reports for detected suspicions events and security violation.

The Physical Security Information Management (PSIM) System and the Incident Management System (IMS) shall be capable of interfacing with the SIEM solution in the Metro System, using standard interfaces such as syslog or equivalent.

SIEM collectors shall be installed in the operational networks. The unidirectional transmission of the SIEM data shall be secured.

The Concessionaire shall establish a process of detecting and monitoring cyber threats on the signalling, systems and networks of the Chennai Metro Project to both the vehicles and the control equipment without disrupting the Chennai Metro Project's proper functioning, and without blocking their communications with the OCC. The Concessionaire shall provide a cyber security dashboard to provide operators with real-time intelligence, forensics and visibility on their Rolling Stock fleet condition and threats.

The Concessionaire shall continuously assess vulnerabilities and weaknesses in the signalling architecture, manages the railway assets and configuration, and offers an effective response to threats in order to mitigate risks.

10.11 System Availability and Continuity

Contingency plans shall be developed, documented and maintained to ensure the essential level of service shall be provided following any loss of processing capability or destruction of IT Systems. All systems shall have Disaster Recovery (DR) .

The system implementation of contingency plans shall not compromise data sensitivity or integrity requirements.

Critical security controls shall be built for resilience and high availability.

Backup – The backup shall maintain the same security policy (confidentiality, integrity and availability) on the backed-up data as on the operational environment. Backups of sensitive data shall have strong encryption and key management. The system shall include the capability to back up and restore all security-relevant data. Processes for secure handling of backup media shall be developed and implemented. Backups shall be kept in at least two separate locations (in addition to the OCC). One of the backup copies shall be kept as an offline backup.

Each environment shall be individually backed-up.

Metro System security shall comply with RAM requirements.

10.12 Technological Means for Security

Security policies, physical means and security systems for preventing unauthorized physical access, damage and interference with the organization's information assets and equipment shall be implemented, before the installation of any active equipment of the following systems: ISS, Communication and IT Systems, P-SCADA, F-SCADA, signaling and CBTC and Security Systems-related equipment and systems.

Refer to the Security Requirements of the Data Centers .

A physical security safeguards shall be implemented in the Metro System facilities. The computer data center shall have physical protections which prevent access by unauthorized personnel.

The appropriate restricted zones for areas shall be established where sensitive IT systems, assets, information and support utilities will be located. These areas include:

a. Data Centers.

b. All the control centers - OCC, NOC, SOC, CSOC.

c. Offices and their related computer equipment.

Access and authorization to the Metro System's zones and premises shall be subject to security and authorization-based business needs and based on segregation of duties.

10.13 Equipment Security

IT equipment shall be protected from theft. Where possible, such equipment shall be locked in racks or secured rooms. Secure table locks shall be implemented for laptops, desktops, monitors or other end user equipment.

Network and Data Center cabinets shall be installed and cabling shall be secured. Communication rooms and rack cabinets shall be locked and equipped with alarm sensors. Manholes and hand holes shall be securely locked. Where they house active communication equipment, they shall be secured with alarm sensors.

11. Security Requirements per Network

The following section provides detailed security requirements applicable to the core networks that are part of the Metro System.

11.1 SCN - Signalling Communication Network

The security elements listed below shall be implemented in the SCN core network:

Strong authentication – including authentication based on token or smartcard, certificates and biometric.

The network layer, which shall be based based on common practice for SCADA and signalling systems (e.g. Purdue model), shall be segregated from the different services of the networks' i.e., it is important to ensure separation between SCADA elements and the VSS elements on the same network.

Authentication of users and equipment shall be implemented through centralized and dedicated mechanism for the network directory service.

User permission shall be based on RBAC mechanism.

Dedicated IT infrastructure for mission critical process control systems shall be implemented.

A dedicated Monitoring system and IDS for the signalling system shall be designed.

A change management mechanism shall be implemented for device configuration monitoring.

Segregation and physical isolation of critical (signalling process control systems) from other networks using a CMRL approved dedicated one-way traffic (data diode type) security device.

The outgoing communications flow between the SCN and the telecommunication backbone network networks, required for proper system functionality, shall be implemented by means of physical one-way traffic enforcement (Diode Type) security device, along with application-level content filtering of the outgoing system messages (by means of data schema enforcement and fields' format and content rules compliance verification, as a minimum).

The SCN shall not include any ingoing communications connections, except a dedicated, one-way connection for application status updates. This connection shall be implemented as a dedicated physical Firewall segment, using a physical one-way traffic enforcement (Diode Type) security device, along with application-level content filtering of the incoming system messages (by means of data schema enforcement and fields' format and content rules compliance verification as a minimum). The application messages format that shall be allowed on this connection is XML only, and any data field transferred through it shall be of a finite enumerated data type, without any usage of strings, binary data blocks and/or unstructured data. The amount of the application interfaces implemented through this connection shall be kept only for the mandatory communication, and each such interface shall be individually submitted to CMRL for approval, after thorough functional necessity analysis.

Each connection in the system shall be based on a solid and valid business case or flow. The list of business cases shall be defined, analyzed and presented as part of the system functional design, for CMRL's approval.

Signalling core network stateful Firewall shall be implemented for networks segmentation.

In addition to all other recording requirements, all sessions to this network shall be recorded.

Remote access to this network, if required, shall be subject to the approval and control of CMRL.

Connection sessions' timeouts shall only be established when the operation does not require permanent connections.

Device control shall be enforced – physical, wireless and removable devices shall be disabled. In addition, sleep mode (i.e., power management state) shall be disabled.

A direct and dedicated link for Maintenance access to network devices or endpoint equipment shall be implemented and performed through dedicated Workstations only.

Unused network ports on devices and equipment shall be disabled.

All unnecessary ports and services at embedded devices shall be disabled.

All built-in system security features shall be enabled.

Download and execution of mobile code (e.g., ActiveX, JavaScript, and VBScript) shall be blocked.

Controlled mediation of information from non-trusted sources such as removable media shall be implemented.

Hard drive locks shall be implemented.

Tamper proof casing of applicable devices and equipment shall be implemented.

Industry recognized Firewalls for Industrial Control Systems (ICS) shall be implemented where applicable compliant with the ISA99 standard.

11.2 Telecommunication Backbone Network – Operational Communication Network

The telecommunication backbone network core network shall have the following security elements implemented, including, but not limited to:

Strong authentication – token based with pin or smartcard, biometric and machine-based certificates.

Authentication of users and equipment shall be implemented through a centralized and network-dedicated Active Directory service.

User permission shall be based on an RBAC mechanism.

Dedicated IT, Networking and security infrastructure shall be implemented.

Safety critical process control systems shall be logically segregated and isolated from other networks using dedicated security devices.

Telecommunication backbone network network traffic with OAIT shall be controlled by security device. The traffic flows shall be permitted on a business needs basis only.

Telecommunication backbone network core network stateful Firewall shall be implemented for networks segmentation.

Remote access (from interfaces external to the BTN) to this network shall be permitted only for compelling operational needs, shall be strictly controlled, and shall be approved in writing by CMRL. The number of users who can obtain access from remote locations shall be limited and justification/approval for such access shall be controlled, documented, monitored and recorded.

Connection sessions' timeouts shall be established only when the operation does not require permanent connections.

Device control shall be enforced – physical, wireless, and removable storages shall be disabled. In addition, sleep mode (i.e., power management state) shall be disabled.

Download and execution of unauthorized mobile code shall be blocked.

Direct link for maintenance access to network devices or endpoint equipment shall be implemented and performed through dedicated Workstations only.

Unused network ports on devices and equipment shall be disabled.

All unnecessary ports and services in embedded devices shall be disabled.

All built-in system security features shall be enabled.

Hard drive locks shall be implemented.

Tamper proof casing of applicable devices and equipment shall be implemented.

Industry recognized Firewalls for Industrial Control Systems (SCADA) shall be implemented where applicable.

Controlled mediation of information from non-trusted sources such as removable media shall be implemented where applicable, compliant with the ISA99 standard.

All unnecessary ports and services in embedded devices such as PLCs and RIU's shall be disabled.

11.3 OAIT – Administrative & Communication Network

The OAIT core network shall have the following security elements implemented, including, but not limited to:

Strong authentication – token based with pin or smartcard and biometric.

Authentication of users and equipment shall be implemented through a centralized and network-dedicated AD service.

User permissions shall be based on an RBAC mechanism.

OAIT network traffic shall by controlled by network Firewall, application Firewall, web proxy servers and anti-malware/anti-spam security devices. The traffic flows shall be permitted on a business needs basis only.

An OAIT core network stateful Firewall shall be implemented for networks segmentation.

Direct link for Maintenance access to network devices or endpoint equipment shall be implemented and performed through authorized Workstations only.

Unused network ports on devices and equipment shall be disabled.

Device control shall be enforced – physical, wireless and removable storages shall be controlled. In addition, features such as auto-run feature (from any connectivity of external authorized devices), sleep mode (i.e., power management state) shall be disabled.

Controlled mediation of information from non-trusted sources such as removable media shall be implemented.

Hard drive locks shall be implemented.

Remote access to the network and resources shall only be permitted providing that authorized users are authenticated, data is encrypted across the network, and privileges are restricted.

Data exchange with external bodies shall take place though a secure platform for managing, sharing and protecting critical information.

12. Security Systems Specific Requirements

12.1 General

As derived from Information Security aspects and operational systems requirements, several separate physical networks shall be implemented as indicated below:

a. Signalling Communication Network (SCN).

b. Operational Communication Network (Telecommunication backbone network).

c. Administrative & Communication Network (OAIT).

The following are specific guidelines for interfacing systems. Security means shall be provided to ensure a secure and accurate system, in full collaboration with other systems suppliers (e.g. external interfaces, GIS, etc.).

12.2 RSS (Railway Scheduling System)

The RSS resides in the OAIT network, which is physically separated from the telecommunication backbone network and SCN networks.

Sharing information between the different networks shall be based on business needs.

Connections between the SCN and any other network (including any required connections between RSS and SCN) shall be implemented according to the requirements described in this document.

The integration between systems shall be permitted only after conducting a risk assessment process followed by a risk management mitigation plan.

12.3 Rolling Stock On-board Systems

As some of the Rolling Stock systems shall be connected to other systems which are not onboard the Rolling Stock, a connection between these systems shall be established. The two relevant separate networks are the SCN and telecommunication backbone network. The connection between these networks shall be protected in order to prevent unauthorized access to the networks.

The commercial network, which is used for Internet access for passengers, shall be completely isolated from the operational and signalling systems. The network separation shall be performed end-to-end, starting with the On-board communication equipment, through the Wideband Wireless Radio System (WWRS/WCDS), to prevent unauthorized access to system resources.

The rolling stock systems which are related to the telecommunication backbone networknetwork shall be separated from the rolling stock systems which are related to the SCN network (in terms of hardware, software and infrastructure). The separation between the networks should be based on a Firewall that will establish an encrypted tunnel which will be connected to a DMZ on the OCC side, and from the DMZ, will be securely connected to the relevant network.

Specific requirements for On-board signalling are provided in the On-board specification document and the WWRS/WCDS, RMCS, as specified in the Communication Systems.

WWRS/WCDS shall provide backup to the RMCS and therefore all ISS restrictions shall apply.

12.4 ATS and SCADA Interface

The ATS is physically separated from the Power SCADA.

One-way information flow (outgoing) shall be permitted to the ATS only by enforcing a unidirectional link (data diode) dedicated security device, approved by CMRL.

Content filter shall be implemented at telecommunication backbone network, based on security gateway/network application firewalling (e.g., content filtering technologies, application gateway firewalls). All information shall be checked for malicious code.

The integration shall be permitted only after conducting a Risk Analysis process and mitigating the risks.

12.5 Interface between Cellular network and Metro CBN (APN/VPN)

In order to allow secured connectivity between mobile devices such as smartphones and tablets to Metro IT systems, a dedicated interface from Cellular (4G/4.5G/5G) public network to the CBN shall be established.

A solution for interfacing the CBN via a 4G/4.5G/5G VPN (provided by one of the authorized carriers in India) shall be provided.

The Chennai Metro Project shall operate an internal cellular core. The project's terminal/mobile devices shall not be able to receive service from commercial cellular providers, and shall be disconnected from the open Internet.

The following are the security requirements regarding this interface:

a. The Metro System authorized and predefined mobile devices shall use an isolated and dedicated APN in the Cellular network.

b. The connection between the Cellular service providers network will be terminated in a dedicated separated physical interface in the telecommunication backbone networkFW.

c. An independent dedicated encrypted tunnel shall be established between the Cellular service provider's data network and the telecommunication backbone network. Users connected to the private APN shall be redirected to the encrypted tunnel

d. A private line for predefined use only: The line shall be used to connect the edge equipment (smartphone or tablet) to the PSIM system from point to point, without additional connections.

e. Mobile edge devices (smartphone/tablet etc.) shall be hardened, and shall ensure the developed application supports the hardening.

13. Security Requirements for Testbed and Pre-Production (Staging) Environment

13.1 Staging

A physically segregated Pre-production (Staging) environment shall be implemented.

The Pre-production environment shall be used for testing IT and OT equipment before its assimilation into the production environment.

The Pre-production environment shall mirror an actual production environment as closely as possible. It shall connect to other production services and data, such as databases.

The primary use of a pre-production environment is to test all the installation/configuration/migration scripts and procedures before they are applied to a production environment. This ensures that all major and minor upgrades to a production environment are completed reliable and free of errors, in a short as possible amount of time.

The staging environment shall be used for performance testing, particularly load testing.

13.2 Testbed and Model

The Concessionaire shall design, install and maintain a systems model of a Hardware, Software and infrastructure-based test environment. Which is coherent with the overall and most updated architecture of the Chennai Metro DC, communication and IT environment.

The entire environment shall be thoroughly examined in several steps on different types of testers prior to its installation and activation in the field.

The test environment shall be a downscaled test platform model of all actual systems and infrastructure for on-board, depot, at-grade, stops and signalling.

The overall examination and assessment of the testbed and model environment, shall constitute the cyber security tests, before its functional activation. .

The objectives of this test environment are to:

a. Approve the goal of protecting data availability, integrity and confidentiality of Chennai Metro Project computing and Information Systems and the resilience of the CBN, systems & subsystems to cyber security attacks.

b. Confirm compliance with cyber security requirements as detailed in this document, complying with CMRL requirements.

c. Test and approve new, updated components before adding them to the production environment.

d. Learning the pattern of actions and forensics capabilities of cyber security events.

Test environment components shall include all systems and subsystems.

Testbed complexes:

a. Test complex.
b. Scenarios complex.
c. Scenarios management complex.
d. Testbed management complex.
e. Debriefing complex.

The testbed model and its components shall be transferred to CMRL after completion of the tests.

The location of the testbed shall be coordinated with and approved by CMRL.

CMRL shall be entitled to carry out testing specifically aimed to detect vulnerabilities in the signaling and CBTC system and/or its components, including all system software components, in its own cyber labs. Alternatively, it may to contract an external testing body for this purpose.

14. Cyber risk Assessment and Penetration Testing

14.1 Periodic Cyber Risk Assessment

The Concessionaire shall conduct an Initial cyber risk assessment prior to the design phase.

The Concessionaire shall periodically (every 24 months as a minimum) conduct a cyber risk assessment in order to assess the capability of an external or an internal hacker to compromise the project systems, network and applications.

The cyber risk assessments shall address multiple points of attacks, including External and internal.

Every cyber risk assessment shall include a detailed report that will include an executive summary, a methodology section, a finding section and a relevant mitigation plan section.

The cyber risk assessment reports shall be submitted to CMRL no later than 30 days after the assessment's execution date.

14.2 Penetration Testing (PT)

The Concessionaire shall periodically conduct a PT (multiple testing) in order to assess the capability of an external or an internal hacker to compromise the project systems, network and applications. The PT shall shall comply with the following requirements:

a. PT for critical components of the Chennai Metro – every 12 months.
b. PT for non-critical components – every 18 months.

In addition, the Concessionaire shall conduct PT prior to PTO, during the trial running of the Metro system.

The PT shall be conducted in coordination with the cyber risk assesment, as specified in section 14.1 above.

Before conducting the PT, the Concessionaire shall present CMRL with the PT scope of work and objective.

The PT shall simulate multiple points of attacks, including External and internal modi operandi.

The PT shall include a detailed report that will include an executive summary, a methodology section, a finding section and a relevant mitigation plan section.

The PT reports shall be submitted to CMRL no later than 30 days after the PT execution date.

ATTACHMENT-03

Key Personnel

Attachment-03

Key Personnel

The Bidder must deploy the key personnel for the positions that meet the following requirements:

No.	Position	Qualification	Nos.	Total Work Experience (Minimum number of years)	Experience in Similar Works (Minimum number of years)
1	Project Manager (PM) – Lifts & Escalators	Graduate in Electrical/ Mechanical Engineering	1	15	10
2	Deputy Project Manager (DPM) - Lifts	Graduate in Electrical/ Mechanical Engineering	1	10	5
3	Deputy Project Manager (DPM) - Escalator	Graduate in Electrical/ Mechanical Engineering	1	10	5
4	Design Engineer – Lifts	Graduate in Electrical/ Mechanical Engineering	1	5	3
		Diploma in Electrical / Mechanical Engineering		10	5
5	Design Engineer – Escalators	Graduate in Electrical/ Mechanical Engineering	1	5	3
		Diploma in Electrical / Mechanical Engineering		10	5
6	Interface Manager *(to be posted at Chennai site from design stage till commissioning of last station)*	Graduate in Electrical/ Mechanical Engineering	1	8	5
7	Project Engineer - Lifts	Graduate in Electrical/ Mechanical Engineering	2	5	3
		Diploma in Electrical / Mechanical Engineering		10	5
8	Project Engineer - Escalators	Graduate in Electrical/ Mechanical Engineering	2	5	3
		Diploma in Electrical / Mechanical Engineering		10	5
9	Installation, Testing & Commissioning Engineer - Lifts	Graduate in Electrical / Mechanical Engineering	2	5	3
		Diploma in Electrical / Mechanical Engineering		10	5
10	Installation, Testing & Commissioning Engineer - Escalators	Graduate in Electrical / Mechanical Engineering	2	5	3
		Diploma in Electrical / Mechanical Engineering		10	5
11	Chief SHE Manager	Graduate in Safety Management	1	10	4
12	Quality Manager	Graduate in Quality Management	1	7	3
13	Civil/Structural Engineer	Graduate in Civil Engineering	1	5	2
		Diploma in Civil Engineering		10	4

The Bidder shall provide details of the proposed personnel and their experience records in Forms PER-1 and PER-2 in Section IV, Bidding Forms.

ATTACHMENT-04

FORM OF PARENT COMPANY UNDERTAKING
&
FORM OF PARENT COMPANY GUARANTEE

Attachment-04

FORM OF PARENT COMPANY UNDERTAKING

THIS UNDERTAKING is made the [ ] day of [ ]
BY[ ] [whose registered office is at]/[of] [ ], together with its successors and assigns, ("the Parent Company"). TO M/S CHENNAI METRO RAIL LIMITED, whose registered office is located at CMRL Depot, Admin. Building, Poonamallee High Road, Koyambedu, Chennai 600 107, INDIA, together with its successors and assigns, ("the Employer").
WHEREAS

(A) By a Contract No. [ ] dated [ ] ("the Contract") made between (1) M/s CHENNAI METRO RAIL LIMITED ("the Employer") and (2) [ ] ("the Contractor"), the Contractor has agreed to design, execute, complete and remedy any defects in the works ("the Works") upon the terms and conditions contained in the Contract.

(B) Pursuant to the terms of the Contract, the Contractor has agreed to procure the provision of an undertaking in the terms hereof.

(C) The Parent Company is the beneficial owner of [ ] % [see Note 1] of the issued share capital of [the Contractor] [see Note 2].

(D) At the request of the Contractor, the Parent Company has agreed to provide this undertaking.

NOW IT IS HEREBY UNDERTAKEN AND AGREED as follows:

1.In consideration of the Employer entering into the Contract with the Contractor, the Parent Company hereby undertakes to the Employer that, the parent company will inform the Employer, in the event, it:

(a) sells, transfers, assigns or otherwise dispose of or deal with ownership of the whole or any part of EITHER [the shareholding or other interest in the [Contractor] [see Note 3] OR [the share holdings or other interests] [see Note 4] referred to in Recital (C) in any way which will affect the beneficial ownership and control in [the Contractor] [see Note 3] of the Parent Company [and the other companies referred to in Recital (C)] [see Note 5]; and

(b) transfers the ownership / control of the subsidiary or of the parent company, an updated Parent Company Guarantee and Parent Company Undertaking will be provided from the new holding/Parent Company.

Further, the Parent Company shall not take any action which may result in the Contractor being unable to comply with his obligations or perform in any way his duties under the Contract [or take any action which may result in [the subsidiary forming part of the Contractor] [see Note 3] being unable to comply with his obligations or perform in any way his duties under the [joint venture or other relevant] agreement] [see Note 6]] until such time as the Works shall have been completed, all the Contractor's obligations under the Contract shall have been performed and the Maintenance and Defects Liability Period (as defined in the Contract) for the whole and every part of the Works shall have elapsed and further that it will ensure [that the subsidiary forming part of the Contractor will take all steps necessary to ensure [see Note 6]] compliance by the Contractor with the provisions of the Contract.
2. The obligations of the Parent Company under this Undertaking shall remain in full force and effect and shall not be affected or discharged in any way and the Parent Company hereby waives notice of: -

(a) any suspension of the Works, variation or amendment to the Contract (including without limitation extension of time for performance) or any concession or waiver by the Employer in respect of the Contractor's obligations [and/or the obligations of [ ] [see Note 7];

(b) any provision of the Contract being or becoming illegal, invalid, void, voidable or unenforceable;

(c) the termination of the Contract or of the employment of the Contractor [and/or]] [see Note 7] under the Contract for any reason;

(d) any forbearance or waiver of any right of action or remedy the Employer may have against the Contractor [and/or [ ]] [see Note 7] or negligence by the Employer in enforcing any such right of action or remedy;

(e) any bond, undertaking, security or other guarantee held or obtained by the Employer for any of the obligations of the Contractor [and/or [ ] [see Note 7] under the Contract or any release or waiver thereof.

3. This Undertaking shall extend to any variation of or amendment to the Contract and to any agreement supplemental thereto agreed between the Employer and the Contractor [and/or [ ]] [see Note 7] and for the avoidance of doubt the Parent Company hereby authorises the Employer and the Contractor [and/or [ ]] [see Note 7] to make any such amendment, variation or supplemental agreement.

4. All documents arising out of or in connection with this Undertaking shall be served:
(a) Upon the Employer, at [ ] marked for the attention of [ ];
(b) Upon the Parent Company, at [ ] India. [Note 8]

5. The Employer and the Parent Company may change their respective nominated addresses for service of documents to another address in India but only by prior written notice to each other. All demands and notices must be in writing.

6. This Undertaking shall be governed by and construed according to the laws for the time being in force in India and the Parent Company agrees to submit to the jurisdiction of the courts in Chennai.

IN WITNESS where of this Undertaking has been executed as a deed on the date first before written.
THE COMMON SEAL of)
[ ])
Was affixed hereto)
In the presence of: -)

Notes: (for preparation of but not for inclusion in the engrossment of this Undertaking)

1. If the Parent Company is not the immediate parent company, the chain of ownership must be recited, identifying each company in the chain and the shareholdings or other interests in each subsidiary.

2. If the Contractor comprises more than one company, that fact and the joint venture or other relevant agreement must be recited. In such case, insert the name of the subsidiary forming part of the joint venture, partnership or consortium, and in respect of which the parent company undertaking is being given.

3. If Note 2 applies, refer to the subsidiary of the Parent Company and not the Contractor.

4.If Note 1 applies, use this alternative.

5.If Note 1 applies, add this provision.

6.If Note 2 applies, add this provision.

7.If Note 2 applies, add this provision and insert the name of the subsidiary.

8.The address for service shall be in India.

ATTACHMENT-04

FORM OF PARENT COMPANY GUARANTEE

THIS GUARANTEE is made the day of
BY [ ] [whose registered office is at]/[of] [ ], together with its successors and assigns, ("the Guarantor").

TO M/S CHENNAI METRO RAIL LIMITED, whose registered office is located at CMRL Depot, Admin. Building, Poonamallee High Road, Koyambedu, Chennai 600 107, INDIA, together with its successors and assigns, ("the Employer").

WHEREAS

(A) By a Contract No.[ ] dated [ ] ("the Contract") made between

1) the CHENNAI METRO RAIL LIMITED ("the Employer") and
2) [ ] ("the Contractor"), the Contractor has agreed to design, execute, complete and remedy any defects in the Works upon the terms and conditions contained in the Contract.

(B) Pursuant to the terms of the Contract, the Contractor has agreed to procure the provision of a guarantee in the terms hereof. [see Note 1].

(C) At the request of the Contractor, the Guarantor has agreed to guarantee performance of the Contract by the [Contractor] [see Note 2] as set out herein.

IT IS HEREBY AGREED AS FOLLOWS:

1. In consideration of the Employer entering into the Contract with the Contractor, the Guarantor irrevocably and unconditionally guarantees to the Employer as a primary obligation and not as a surety due performance by the [Contractor] [see Note 2] of all of its obligations and liabilities under and in accordance with the Contract save that nothing herein shall be construed as imposing greater obligations or liabilities on the Guarantor than are imposed on the [Contractor] [see Note 2] in the Contract.

2. The obligations of the Guarantor under this Guarantee shall remain in full force and effect and shall not be affected or discharged in any way by and the Guarantor hereby waives notice of:-

(a) any suspension of the Works, variation to or amendment of the Contract (including without limitation extension of time for performance) or any concession or waiver by the Employer in respect of the Contractor's obligations [and/or the obligations of [ ] [see Note 3] under the Contract;

(b) any provision of the Contract being or becoming illegal, invalid, void, voidable or unenforceable;

(c) the termination of the Contract or of the engagement of the Contractor [and / or [....]] [see Note 3] under the Contract for any reason;

(d) any forbearance or waiver of any right of action or remedy the Employer may have against the Contractor [and / or [....]] [see Note 3] or negligence by the Employer in enforcing any such right of action or remedy;

(e) any bond, undertaking, security or other guarantee held or obtained by the Employer for any of the obligations of the Contractor [and / or [.....] [see Note 3]under the Contract or any release or waiver thereof.

3. This Guarantee shall extend to any variation of or amendment to the Contract and to any agreement supplemental thereto agreed between the Employer and the Contractor [and/or] [see Note 3] and for the avoidance of doubt the Guarantor hereby authorises the

Employer and the Contractor [and/or [ ]] [see Note 3] to make any such amendment, variation or supplemental agreement.

4. This Guarantee is a continuing guarantee and accordingly shall cover all of the obligations and liabilities of the [Contractor] [see Note 2] under the Contract and remain in full force and effect until all the said obligations and liabilities of the Contractor shall have been carried out, completed and discharged in accordance with the Contract. This Guarantee is in addition to any other security which the Employer may at any time hold and may be enforced without first having recourse to any such security or taking any steps or proceedings against the Contractor.

5. Until expiry of the Maintenance and Defects Liability Period (as defined in the Contract) for the whole and every part of the Works, the Guarantor shall not on any ground whatsoever make any claim or threaten to make any claim whether by proceedings or otherwise against the Contractor [and/or [ ]] [see Note 3] for the recovery of any sum paid by the Guarantor pursuant to this Guarantee. Any such claim shall be subordinate to any claims (contingent or otherwise) which the Employer may have against the Contractor [and/or [ ]] [see Note 3] arising out of or in connection with the Contract until such time as such claims shall be satisfied by the Contractor [and/or [ ]] [see Note 3] or the Guarantor as the case may be. To that intent the Guarantor shall not claim or have the benefit of any security which the Employer holds or may hold for any monies or liabilities due or incurred by the Contractor [and/or [ ]] [see Note 3] to the Employer and, in case the Guarantor receives any sum from the Contractor [and/or [ ]] [see Note 3] in respect of any payment by the Guarantor hereunder, the Guarantor shall hold such sum in trust for the Employer for so long as any sum is payable (contingently or otherwise) under this Guarantee.

6. The Employer shall be entitled to assign the benefit of this Guarantee at any time without the consent of the Guarantor or the [Contractor] [see Note 2] being required.

7. All documents arising out of or in connection with this Guarantee shall be served:

(a) Upon the Employer, at [ ], marked for the attention of [ ];

(b) Upon the Guarantor, at [ ] India [Note 4]

8. The Employer and the Guarantor may change their respective nominated addresses for service of documents to another address in India but only by prior written notice to each other. All demands and notices must be in writing.

9. This Guarantee shall be governed by and construed according to the laws for the time being in force in India and the Contractor agrees to submit to the jurisdiction of the courts of India at Chennai.

IN WITNESS whereof this Guarantee has been executed as a deed on the date first before written.

THE COMMON SEAL of)

[ ])

Was affixed hereto in)

The presence of: -)

Notes (for preparation of but not inclusion in the engrossment of this Guarantee):

1. *If the Contractor comprises more than one company, that fact, the joint venture or other relevant agreement and the relationship of the Guarantor to its subsidiary forming part of the Contractor must be recited.*

2. *If Note 1 applies, replace the word "Contractor" with name of the subsidiary being guaranteed.*

3. *If Note 1 applies, add additional wording and insert the name of the subsidiary being guaranteed.*

4. *The address for service shall be in India.*

ATTACHMENT-05

Condition Based Monitoring (CBM) for Escalators

Attachment-05

6.12 Condition Based Monitoring (CBM) for Escalators

Predictive Maintenance: The ability to view the escalators in real time and monitor its current performance against the optimum performance set at the time of test, (i.e., in good health) this would be invaluable in terms of predicting deterioration. CBM is used to record the status of individual components in order to provide a more predictive approach to effective component lifespan and projected failure. Following are the minimum I/O points shall be monitored for Escalators. Contractor has to review for the required Hardware and Sensors which are required for the same. The details shall be reviewed during design stage.

Escalators:

a. Speed profile including constant monitoring of acceleration, top speed and deceleration and the optimum speed curves
b. Incoming voltage and current
c. Bearing Temperature
d. Temperature of Control Cabinet for traction winding unit with gear oil
e. Power usage
f. Motor displacement status
g. Safety sensors status
h. Pit Float sensor/switch status
i. Overheating inside the escalators
j. Major safety parameter status
k. Handrail Speed/safety fault status
l. Auto cut off sensor status
m. Controller status

ATTACHMENT-06

Subcontractors/manufacturers

Attachment-06

12.20 Subcontractors/manufacturers

Subcontractors/manufacturers for the following major items of supply or services must meet the following minimum criteria, herein listed for that item:

Item No.	Description of Item	Minimum Criteria to be met
A	**Lifts**	
1	Motor	Units provided: 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
2	VVVF Drive	Units provided: 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
3	Speed Governor	Units provided: 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
4	Safety Gear	Units provided: 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
5	Landing & Car Door Assembly	Units provided: 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
6	3D Infra-Red Sensor	Units provided: for 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
7	Suspension Rope/ Belt	Units provided: for 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
8	Car & Counterweight Guide Rails	Units provided: for 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
9	Steel & Structural Steel	Units provided: for 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
10	Glass	Units provided: for 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
11	All Cables	Units provided: for 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
12	Stainless Steel	Units provided: for 40 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).

Item No.	Description of Item	Minimum Criteria to be met
B	**ESCALATORS**	
1	Motor	Units provided: 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
2	VVVF Drive	Units provided: 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
3	Gearbox Assembly	Units provided: 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
4	Chains & Sprockets (Main Drive & Step)	Units provided: 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
5	Handrail	Units provided: 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
6	Step & Chain Rollers	Units provided: for 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
7	Steps	Units provided: for 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
8	Steel & Structural Steel	Units provided: for 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
9	Glass	Units provided: for 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
10	All Cables	Units provided: for 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
11	Stainless Steel	Units provided: for 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).
12	Sensor & Limit switch	Units provided: for 90 nos. with a minimum of 3 years in satisfactory operation in Mass Rapid Transit System (Metro, Airports, Sub-Urban Railways, Railways etc.).

Failure to comply with this requirement will result in rejection of the Subcontractor.

In the case of a Bidder who offers to supply and install major items of supply under the Contract that the Bidder did not manufacture or otherwise produce, the Bidder shall provide the manufacturer's authorization, using Form MAN provided in Section IV, Bidding Forms, showing that the Bidder has been duly authorized by the manufacturer or producer of the related plant and equipment or component to supply and install that item in the Employer's country. The Bidder is responsible for ensuring that the manufacturer or producer complies with the requirements of ITB 4 and ITB 5 and meets the minimum criteria listed above for that item.

ATTACHMENT-07

PROJECT MANAGEMENT INFORMATION SYSTEM (PMIS)

Attachment-07

1. PROJECT MANAGEMENT INFORMATION SYSTEM (PMIS)

1.1 The Employer is presently in negotiations to provide a PMIS which is going to be a web based platform on cloud to monitor and track the progress of the whole project, tailored to match the specific needs of the project.

2.1 The aim is to provide the Employer and the Engineer with insights critical for the smooth and timely execution of the project. The Contractor will be required to submit the data and information for the PMIS as described by the Engineer.

3.1 The contractor once awarded the contract will develop a Method Statement for the control of document and management information as per the requirements of chosen system in co-ordination with the Engineer which shall also detail various processes of the PMIS.

4.1 The information shall include but shall not be limited to:

(1) Schedule related information

(2) Progress related information

(3) Issues related to the project

(4) Safety related information

(5) Quality related information

5.1 The integrated system will also take inputs from Primavera and project the possible delays and achievements of the various Contractors and also the overall project. The management team can review the overall health and synopsis of the entire project on the master dashboard.

6.1 The contractor will be managing the PMIS for entire contract duration including the defects liability period for their contract package including sharing the proportionate cost of

- Cloud based server (The Employer will be acquiring the common cloud based server for all contract packages of phase 2 and back charge the proportionate cost of the Server, Cloud services and the manage services of the cloud server to each contractor.
- 3 nos user licenses cost for Primavera P6 Enterprise Project Portfolio Management Cloud Service 1 No. each to be used by the Contractor, the Engineer and the Employer. Please note that the Contractor can ask for more licenses if he wish to but strictly on his cost
- 3 nos user licenses cost for Project Management Software to be procured for 1 No. each to be used by the Contractor, the Engineer and the Employer. Please note that the Contractor can ask for more licenses if he wish to but strictly on his cost.
- The Employer will be hiring a professional agency to implement P6 EPPM for whole project and integrate it with PMIS. The contractor for each package will have to share proportionate cost for their package. Any other software required to interact with PMIS for their contract package needed to update the information as explained above.

2. Document Management System

PMIS, which will be containing, amongst many other modules, a module on document management system, such that all documents generated by the Project and Interface Contractors can be transmitted to the Employer and the Engineer, by electronic means, and vice versa, and that all documents generated by all parties are electronically captured at the point of origin and can be reproduced later, electronically and in hard copy. The Contractor shall note that a limited number of his staff will receive specific training in the use of the PMIS system, which shall be organised by the Employer at a time and location yet to be determined.

The number and format of the required document submissions is detailed in Attachment A1 to this Section. The Transmittal Form is given in Attachment A2 to this Section A and the Document Submission Report, for the obtaining of a Notice of No Objection from the Engineer, is given in Attachment A3 to this Section.

7.1 The Method Statement for the control of document and management information to be submitted by the Contractor shall also detail the uploading, maintaining, and archiving the following submittals, included but not limited to:

(1) Contractual Works Programmes, Work Segment Programmes, and supporting reports (including plans) as per the format and using the software as defined in the Contract,

(2) Drawings (including As build drawings), BIM Models and designs created by the Contractor as per the construction asset (classification) and on the software platform defined in the Contract,

(3) Records of measurement or Contractor’s Statements or both, in a format defined in the Contract,

(4) Construction asset details needing to be updated in the Contractor’s Monthly Progress Reports,

(5) Geo-referencing of the alignment,

(6) Geo-referencing co-ordinates of assets into a geographic information system (GIS) which the Contractor’s Monthly Progress Report has utilised,

(7) Contractor’s Monthly Progress Reports, and

(8) Source files for submittal as required by the Engineer.

The Contractor is required to assess the entire cost associated with all above requirements and include the same in his quoted price.

ATTACHMENT A1

	No. of Paper Copies			No. of Electronic Copies	Reference
	A1	A3	A4		
Initial Programme and Works Programme plus supporting information and narrative		6		2	
Monthly Programme Update		6		2	
Three Month Rolling Programme		6		2	
Three Week Rolling Programme		6		2	
Monthly Progress Report			6	2	
Working Drawings / Shop Drawings	3	3		2	
Method Statements			3	2	
Interface Management Plan			3	2	
As Built Drawings	3	3	3	2	
Materials Submissions (documentation)			3	2	
Quality Plan			3	2	
Quality Control Register			3	2	
Reports of Quarterly Quality Audits			3	2	
Materials and Workmanship Test Results/Reports			3	2	
Safety Plan			3	2	
Environmental Plan			3	2	
Traffic Management Submissions		3		2	
Investigation and survey reports.			3	2	
Monitoring, protection and replacement proposal reports.		3		2	
All other submittals		3		2	As applicable

Required Number of Copies of Submittals and Format Requirements

Notes :

i) In case of any contradiction between the text and this table then the text shall prevail, unless otherwise instructed by the Engineer.

ii) Drawings to support A4 text documents shall be of A3 size.

ATTACHMENT A2

TRANSMITTAL FORM

Chennai Metro Rail Limited
TRANSMITTAL FORM

CONTRACTOR		EMPLOYER'S REPRESENTATIVE
NAME:	TRANSMITTAL REF No.:	NAME:
CONTRACT No:	DATE OF SUBMISSION:	
SIGNATURE:		

We submit;

- ☐ Plans
- ☐ Work plan & methodology
- ☐ Design criteria, studies
- ☐ Calculations
- ☐ Drawings
- ☐ Specifications
- ☐ B.O.Q
- ☐ Report
- ☐ Prints
- ☐ Samples
- ☐ Seperately via _____
- ☐ Items(to specify) _____
- ☐ Other(to specify): _____

Stage of submission:

- ◉ Design
- ○ Execution
- ○ Tests

SUBJECT:			
Date of document	**No. of Copies**	**Document reference**	**Revision**

These are transmitted as checked below :

- ☐ For your information
- ☐ First submission for Notice of No Objection
- ☐ Resubmission with corrections for Notice of No Objection
- ☐ Other(to specify) _____

REMARKS

ISSUING ENTITY :

The document (s) hereby submitted have been properly reviewed according to our QA system, to confirm its completeness, accuracy, adequacy and validity.

Signature:

Name: | Date:

COPY TO:

ACKNOWLEDGMENT OF RECEIPT :

Signature:

Name: | Date:

File Reference: FQAC-49-A

Page 1/1

Chennai Metro Rail Limited

DOCUMENT SUBMISSION REPORT (DSR) - STATUS SHEET

ORIGINATOR
(•) ENGINEER ( ) CMRL

No of Contract:		DSR Code	
Reference of Letter/Transmittal		Discipline:	
Reception date of Letter/Transmittal		Assessor:	
		Discipline Coordinator:	
		Prepared by Team Leader:	

SUBJECT:

List of documents submitted

N°	Document reference	Revision	Date	Notification		
				A	B	C
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						

Notification

Definition of notification:
A. Objection. A complete resubmission is required
B. No Objection with comments.
C. Notice of No Objection

Area of Deficiency	Comment Items No (Note)

Repeated Comments	New Comments

No of Comments in PR	No of Comments in NS

PR=Partial Resubmission; NS=Next Submission

Discipline Team Leader

Printed name	Position	Date	Signature

The comments are given to ensure the submission conforms to the Contract provisions.

File Reference: FOAC-34-B

CHENNAI METRO RAIL PROJECT
DOCUMENT REVIEW SHEET **(DRS)**

NKAB

SUBMITTAL - DETAILS

Document/Drawing Submitted by		Contract Reference	
Submittal Document No.		DRS Reference	
Submittal Name		DRS Revision No.	R0
Date of Submittal Received		Date Issued	
PMIS/Transmittal Reference		DRS Owner	

Severity of the Comments	Major: will attribute to Rejected Status Moderate: will attribute to NOWC Status Minor: will attribute to NOWC Status		Status Awarded		Comment Status by Engineer
Item	Doc/Drg/Section/ Page	Reviewer`s Comments	Reviewer Initials	Severity	Submitter's Response	
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						

Notes:
1. The acceptance of these documents by Engineer /Employer shall not be deemed as validation of your submission and nor does it infer their fitness for the purpose. Engineer / Employer does not accept any liability for the submission.
2. Any changes to the documents should be undertaken in accordance with your organization's approved change control procedures.
Such variations must be formally recorded and evidence should accompany any resubmission.
3. Without relieving the originating organization of their contractual responsibilities, the status codes for each document are provided after review.
4. Whenever any change occurs that invalidates the information contained in the previously submitted and reviewed document, within 14 days of the occurrence of such change; and when requested by the Engineer from time to time
5. This DRS Report is part of the Drawing/Document and shall be kept in the last pages of drawing/Document.
6. The Engineer's opinion on the status of the comments or the overall status of the DRS is final.
7. The status of document shall not in any way imply any change to the Contract price or Time for Completion.

Disclaimer : Permission to proceed shall not constitute acceptance or approval of design details, calculations, analyses, test methods or materials developed or selected by the Contractor and shall not relieve the Contractor from full compliance with Contractual obligations.

This DRS document is invalid unless it is signed off by all people (as applicable) in all pages	Signature	Signature		DC to circulate signed PDF along with Native file to the Contractor
	Reviewed by (Engineers/Architects)	Checked by (DREs/Experts/Sr. Managers)	Issued by (CREs/Chief Experts/CM/DTL)	

ATTACHMENT-08

General Experience

Clause No. 2.4.1 General Experience:

Eligibility and Qualification Criteria			Compliance Requirements				Documentation
No.	Factor /Sub-Factor	Requirement	Single Entity	Joint Venture (Existing or Intended)			Submission Requirements
				All Parties Combined	Each Member	Lead Member	
2.4 Experience							
2.4.1	**General Experience**	Experience under Lifts & Escalators contracts in the role of prime contractor (single entity or JV member) for at least the last **FIVE (05)** years starting **1st January 2016.**	Must meet requirement	Must meet requirement	N/A	N/A	Form EXP - 1

Replaced as

Eligibility and Qualification Criteria			Compliance Requirements				Documentation
No.	Factor /Sub-Factor	Requirement	Single Entity	Joint Venture (Existing or Intended)			Submission Requirements
				All Parties Combined	Each Member	Lead Member	
2.4 Experience							
2.4.1	**General Experience**	Experience under Lifts & Escalators contracts in the role of prime contractor (single entity or JV member) for at least the last **FIVE (05)** years starting **1st January 2016.**	Must meet requirement	**N/A**	**Must meet requirement**	N/A	Form EXP - 1

ATTACHMENT-09

Price Centre "A1" - Preliminaries and General Requirements

PRICE CENTRE 'A1' – PRELIMINARIES AND GENERAL REQUIREMENTS:				
Price Centre	**Item Description**	**Unit**	**Qty**	**% of sub items**
Obtain Notice of No Objection from the Engineer/Employer for:				
A1.	**Preliminaries and General Requirements**			
A1.1	**Contractual Submissions (Submission of PII, Bond, Insurances, etc.)**			
A1.1.1	Submission of PII, Bond, Insurances, CAR policy, Performance BG etc.	Item	1	4%
A1.2	**General Items**			
A1.2.1	Initial Works Programme	Item	1	4%
A1.2.2	Detailed Works Programme, Updates, revisions and Three Month Rolling Programme	Quarterly	12	5%
A1.2.3	Monthly Progress Report	Monthly	36	4%
A1.2.4	Interface Management Plan and Audits - Quarterly	Quarterly	12	5%
A1.2.5	Interface Matrix and Specific Contract Interface Sheets	Item	1	4%
A1.2.6	All interface management and coordination, including provision of services for the interfacing Contractors	Quarterly	12	5%
A1.2.7	Interface management and coordination from the issue of Taking Over Certificate/Handover until start of Revenue Services. (Employer to instruct if required)	No.	8	4%
A1.2.8	Various Programs throughout the Contract by Project Management Information Systems	Monthly	36	5%
A1.2.9	System Safety Plans and audits-Quarterly	Quarterly	12	4%
A1.2.10	Contractor's Staff and Organization Plan & Key Staff (Key staff payment deduction in case of non-deployment or delay in deployment, refer Part 1 – Bidding Forms).	Monthly	36	3%
A1.2.11	OHS&E Posters and Plans as per OHS&E Manual as per Employer's requirements	Monthly	36	3%
A1.2.12	Construction Phase Safety Plan etc. submission refer clause No: 4.4.6.2 of OHS&E Employer's requirements	No.	1	2%

A1.2.13	Audit (refer the clause No: 4.5.5) & ISO Certifications refer clause No: 4.3.3.2 of OHS&E Employer's Requirements			
	Monthly Audit report (MARS): 90%	Quarterly	12	7%
	International Certification to ISO 45001:2018 and ISO 14001:2015 standard:10%	Item	1	2%
A1.2.14	OHS&E Training refer the clause No: 4.4.2.2 and Quarterly OHS&E Audit refer clause No: 4.5.5.2 of OHS&E Employer's Requirements			
	Training Implementation: 50%	Monthly	36	3%
	Quarterly Audit: 50%	Quarterly	12	3%
A1.2.15	Environmental Management Plan & Audits Quarterly	Quarterly	12	3%
A1.2.16	Construction and Maintenance of Employer's/ Engineer's Site office as per Employer's Requirement	Quarterly	12	4%
A1.2.17	Reliability, Availability, Maintainability Safety (RAMS) plans	Quarterly	12	4%
A1.2.18	Comprehensive Installation, Testing and Commissioning Programme and Equipment wise Schedule	Quarterly	12	5%
A1.2.19	Submission of Complete BIM Model (As Built).	Quarterly	12	4%
A1.2.20	Submission of Maintenance Plans for CAMC as per Employers Requirements	Quarterly	28	5%
A1.2.21	PMIS as per Employers Requirements	Quarterly	40	3%
A1.2.22	Any other item(s) considered necessary to comply with the scope of Works.	Item		5%
	Total for Price Center A1	----	----	**100%**

Validate | Print | Help

Tender Inviting Authority: CHENNAI METRO RAIL LIMITED

Name of Work: "Design, Manufacture, Supply, Installation,Testing & Commissioning of Heavy Duty Machine Room Less Lifts and Escalators"

Tender No: C4-AES-05-L&E

Name of the Bidder/ Bidding Firm / Company :	

PRICE SCHEDULE

(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevent columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)

NUMBER #	TEXT #	TEXT #	NUMBER #	NUMBER	NUMBER	NUMBER	NUMBER	TEXT	TEXT	NUMBER	NUMBER	NUMBER	NUMBER	TEXT	NUMBER	NUMBER	NUMBER #	TEXT #
Sl. No.	Currency (Ref ITB 19.1)	Quoted Currency in INR / Other Currency	Price Centre A1: Preliminaries and General Requirements 3.50%	Price Centre A2: Installation, Testing & Commissioning Manuals and Operation & Maintenance (O&M) Manuals 0.50%	Price Centre A3: Training for Employer's personnel 1.00%	Price Centre A4: Complete Definitive Design including Prototype and Type Test 3.00%	Price Centre B1: Lifts in Stage 1 and Stage 2 Stations (To be carry forwarded from BOQ 'B1') 80.00%	Price Centre B2: Escalators in Stage 1 and Stage 2 Stations (To be carry forwarded from BOQ 'B2') 80.00%	Price Centre C1: Comprehensive Annual Maintenance (CAMC) Services for Stage 1 stations during Defect Notification period of 2 Years. (To be carry forwarded from BOQ 'CAMC') 1.3%	Price Centre C2: Comprehensive Annual Maintenance (CAMC) Services for Stage 2 stations during Defect Notification period of 2 Years. (To be carry forwarded from BOQ 'CAMC') 0.7%	Price Centre C3: Comprehensive Annual Maintenance (CAMC) Services for Stage 1 and Stage 2 stations for 5 years beyond Defect Notification period. (To be carry forwarded from BOQ 'CAMC') 10.00%	Total Amount in INR (In addition to selected foreign currency) (INR)	Lumpsum Price for Corridor 4 – Lifts & Escalators for the entire scope of works covered under Part 2 – Employer's Requirements (C4-AES-05-L&E)	Discount (if any) – Applicable on Lumpsum price %	Lumpsum Price (C4-AES-05-L&E) after discount	Provisional Sum (Not included for evaluation)	TOTAL AMOUNT, (Lumpsum Price after discount if any + Price Centre G + Price Centre H) It will be converted to equivalent INR as per ITB 37.1	TOTAL AMOUNT In Words
1	2	12	13	14	15	16	17	18	19	20	21	22	23	24	26	29	53	55
1.01	Indian Rupees	INR		4.00	6.00	8.00	0.00	0.00	0.00	0.00	0.00	0.00	18.00		18.00	20000000	18.00	INR Eighteen Only
1.02	Foreign Currency 1	USD		4.00	6.00	8.00	0.00	0.00	0.00	0.00	0.00		18.00		18.00		18.00	USD Eighteen Only
1.03	Foreign Currency 2	EUR		4.00	6.00	8.00	0.00	0.00	0.00	0.00	0.00		18.00		18.00		18.00	EUR Eighteen Only

Validate | Print | Help

Item Wise BoQ

Tender Inviting Authority: Chennai Metro Rail Limited

Name of Work: "Design, Manufacture, Supply, Installation,Testing & Commissioning of Heavy Duty Machine Room Less Lifts and Escalators"

Contract No: C4-AES-05-L&E

Name of the Bidder/ Bidding Firm / Company :	

PRICE SCHEDULE

(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevent columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)

Note:

(1). The Bidder can quote in local currency (INR) or any one Foreign Currency of USD or EUR.

(2). The bidder who wishes to quote rates in multiple currency (INR with USD/EUR) for a single item, first select "partial conversion" in column no:11 and carefully select the foreign currency (USD/EUR) from column No.12 and insert rate in foreign currency in Column No.13. Additional Indian currency (INR) shall be inserted in Column No.14"

NUMBER #	TEXT #	NUMBER #	TEXT #	TEXT#	TEXT #	NUMBER #	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER #	NUMBER #
Sl. No.	Item Description	Total Quantity	Door Opening (Same side /Through Car)	Currency Convertion against each Item	Quoted Currency in INR / Other Currency	Unit rate as per selected currency in column No.12 - (INR/USD/ EUR)	Unit rate in INR only (to be quoted if required in addition to selected foreign currency in column No.12)	TOTAL AMOUNT in (INR)	TOTAL AMOUNT in FC1 Select Currency in Drop dropdown list (USD)	TOTAL AMOUNT in FC2 Select Currency in Drop dropdown list (EUR)	Total amount in INR from column No.14	TOTAL AMOUNT, It will be converted based on coloumn L	TOTAL AMOUNT in INR
1	2	4	5	11	12	13	14	15	21	22	23	53	54
1.00	PRICE CENTRE B1							INR	USD	EUR	INR		
2.00	Lifts in Stage 1 and Stage 2 Stations (A. 13 P/1000 Kg Lifts)												
3.00	Upto 7 metre Travelling Height- 2 stops	48.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
4.00	From 8 metre to 12 metre Travelling Height - 2 stops	19.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
5.00	From 8 metre to 12 metre Travelling Height - 2 stops	4.00	Through Car	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
6.00	From 8 metre to 12 metre Travelling Height - 3 stops	8.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
7.00	From 8 metre to 12 metre Travelling Height - 3 stops	2.00	Through Car	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
8.00	From 13 metre to 17 metre Travelling Height - 2 stops	2.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
9.00	From 13 metre to 17 metre Travelling Height - 2 stops	1.00	Through Car	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
10.00	From 13 metre to 17 metre Travelling Height - 3 stops	1.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
11.00	From 18 metre to 23 metre Travelling Height - 2 stops	4.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
12.00	From 18 metre to 23 metre Travelling Height - 4 stops	3.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
13.00	From 18 metre to 23 metre Travelling Height - 4 stops	2.00	Through Car	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
14.00	B. Lifts in Stage 1 and Stage 2 Stations - 26P/1800 Kg												
15.00	Upto 7 metre Travelling Height - 2 stops	1.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
16.00	From 8 metre to 12 metre Travelling Height - 2 stops	11.00	Same Side	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
17.00	From 8 metre to 12 metre Travelling Height - 2 stops	1.00	Through Car	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
Total in Figures								0.00	0.00	0.00	0.00	0.00	0.00

Validate | Print | Help

Item Wise BoQ

Tender Inviting Authority: Chennai Metro Rail Limited

Name of Work: "Design, Manufacture, Supply, Installation,Testing & Commissioning of Heavy Duty Machine Room Less Lifts and Escalators"

Contract No: C4-AES-05-L&E

Name of the Bidder/ Bidding Firm / Company :	

PRICE SCHEDULE

(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevent columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)

Note:

(1). The Bidder can quote in local currency (INR) or any one Foreign Currency of USD or EUR.

(2). The bidder who wishes to quote rates in multiple currency (INR with USD/EUR) for a single item, first select "partial conversion" in column no:11 and carefully select the foreign currency (USD/EUR) from column No.12 and insert rate in foreign currency in Column No.13. Additional Indian currency (INR) shall be inserted in Column No.14"

NUMBER #	TEXT #	NUMBER #	TEXT #	TEXT#	TEXT #	NUMBER #	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER	NUMBER #	NUMBER #
Sl. No.	Item Description	Total Quantity	Units	Currency Convertion against each Item	Quoted Currency in INR / Other Currency	Unit rate as per selected currency in column No.12 - (INR/USD/ EUR)	Unit rate in INR only (to be quoted if required in addition to selected foreign currency in column No.12)	TOTAL AMOUNT in (INR)	TOTAL AMOUNT in FC1 Select Currency in Drop dropdown list	TOTAL AMOUNT in FC2 Select Currency in Drop dropdown list	Total amount in INR from column No.14	TOTAL AMOUNT, It will be converted based on coloumn L	TOTAL AMOUNT in INR
1	2	4	5	11	12	13	14	15	21	22	23	53	54
1.00	PRICE CENTRE B2							INR	USD	EUR	INR		
2.00	Escalators in Stage 1 and Stage 2 Stations												
3.00	3.0 Meter Vertical Rise Stainless Steel Balustrade:-	4.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
4.00	3.0 Meter Vertical Rise Glass Balustrade:-	2.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
5.00	4.0 Meter Vertical Rise Stainless Steel Balustrade:-	10.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
6.00	4.0 Meter Vertical Rise Glass Balustrade:-	24.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
7.00	5.0 Meter Vertical Rise Stainless Steel Balustrade:-	9.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
8.00	6.0 Meter Vertical Rise Stainless Steel Balustrade:-	8.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
9.00	6.0 Meter Vertical Rise Glass Balustrade:-	22.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
10.00	7.0 Meter Vertical Rise Stainless Steel Balustrade:-	34.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
11.00	7.0 Meter Vertical Rise Glass Balustrade:-	41.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
12.00	8.0 Meter Vertical Rise Stainless Steel Balustrade	14.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
13.00	8.0 Meter Vertical Rise Glass Balustrade	10.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
14.00	9.0 Meter Vertical Rise Stainless steel Balustrade	9.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
15.00	10.0 Meter Vertical Rise Stainless Steel Balustrade	2.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
16.00	12.0 Meter Vertical Rise Glass Balustrade:-	4.00	Nos	Full Conversion	INR			0.00	0.00	0.00	0.00	0.00	0.00
Total in Figures								0.00	0.00	0.00	0.00	0.00	0.00

Validate | Print | Help

Item Wise BoQ

Tender Inviting Authority: Chennai Metro Rail Limited

Name of Work: "Design, Manufacture, Supply, Installation,Testing & Commissioning of Heavy Duty Machine Room Less Lifts and Escalators"

Contract No: C4-AES-05-L&E

Name of the Bidder/ Bidding Firm / Company :	

PRICE SCHEDULE

(This BOQ template must not be modified/replaced by the bidder and the same should be uploaded after filling the relevent columns, else the bidder is liable to be rejected for this tender. Bidders are allowed to enter the Bidder Name and Values only)

NUMBER #	TEXT #	NUMBER #	TEXT #	NUMBER	TEXT #	NUMBER #	NUMBER	NUMBER	NUMBER
Sl. No.	Item Description	Period (Quarterly)	Units	Total Quantity	Quoted Currency in INR / Other Currency	Unit rate of Respective Item	TOTAL AMOUNT in INR	TOTAL AMOUNT in FC1 Select Currency in Drop dropdown list	TOTAL AMOUNT in FC2 Select Currency in Drop dropdown list
1	2	4	5	6	12	13	14	21	22
1.00	PRICE CENTRE 'C1', 'C2', 'C3'						INR	USD	EUR
2.00	Comprehensive Annual Maintenance Contract (CAMC) for Lifts & Escalators in Corridor 4 - Stage 1 and Stage 2 Stations – BOQ 'CAMC'								
3.00	**C1. Comprehensive Maintenance (CAMC) Services for Stage 1 Stations during Defect Notification Period (DNP) of 2 Years**								
4.00	Lifts	8.00	Nos	74.00	INR		0.00	0.00	0.00
5.00	Escalators	8.00	Nos	118.00	INR		0.00	0.00	0.00
6.00	**C2. Comprehensive Maintenance (CAMC) Services for Stage 2 Stations during Defect Notification Period (DNP) of 2 Years**								
7.00	Lifts	8.00	Nos	33.00	INR		0.00	0.00	0.00
8.00	Escalators	8.00	Nos	75.00	INR		0.00	0.00	0.00
9.00	**C3. Comprehensive Annual Maintenance (CAMC) Services for Stage 1 and Stage 2 Stations for 5 years beyond Defect Notification period (DNP).**								
10.00	Lifts	20.00	Nos	107.00	INR		0.00	0.00	0.00
11.00	Escalators	20.00	Nos	193.00	INR		0.00	0.00	0.00
Total in Figures							0.00	0.00	0.00