Addendum-03
CMRL/PHASE -II/SYS/CP22/ASA04/2021
01 March 2022

SN	Part	Section	Clause	Original Bid condition	Revised bid condition
1	Part 1	Section IV - Bidding Forms	4.1.7	Wherever the Bidder comprises a JV/Consortium and the Bidder desires separate payments to each Member of the Consortium, the Bidder shall clearly lay down the Milestones / Currencies allocated to the different Members of the JV/Consortium, which shall be in agreement with the intended percentage share of the Members as indicated in the Consortium agreement for this Contract.	Whenever the bidder comprises of a Single Entity / JV Bidder, Payment will be made only to Bank Account of Single Entity / JV. In case of Consortium Bidder, and where the Bidder desires separate payments to each member of the Consortium, Payment to individual members will be made upon submission of seperate Invoices by Consortium members through Lead member. In such case, the Bidder shall clearly lay down the Milestones / Currencies allocated to the different members of the Consortium, which shall be in agreement with the intended percentage share of the members as indicated in the Consortium agreement for this Contract.
2	Part 1	Section IV - Bidding Forms	4.2.2		Note: (1) 'Price Centre K' (Training and Operation & Maintenance Manual) and 'Price Centre L' (Contract Spares, Special tools, Testing Equipments, Measuring Instruments and Maintenance assistance) will be auto filled in CPP e-procurement portal based on predefined apportionment percentage against the same, upon filling the Lumpsum price (Signalling and Train Control System) in Excel Price Bid Form. (2) In addition, Bidders have to upload the duly filled 'BOQs for Price Centre K and L' as per Cl. 4.2.1 and 4.2.2 above respectively, along with 'Letter of Price Bid' as part of Financial bid only. These BOQs strictly should not be uploaded as part of Technical bid. Bidders have to ensure that the Total amount of 'BOQs for Price Centre K and L' shall be in line with the value of Price Centre K and Price Centre L quoted by the Bidder in Excel Price bid form. (3) In case of any deviation between value of 'Price Centre K and L' as in Excel Price Bid form and total amount of 'BOQs for Price Centre K and L', the quoted value by the Bidder in Excel Price Bid form shall prevail and the BOQs for Price Centre K and L' shall be appropriately readjusted by the Employer in line with the quoted value by the Bidder in Excel Price bid form, before entering into the Contract agreement.
3	Part 1	Section IV - Bidding Forms	4.3.1, 4.3.2	DETAILS NOT TO BE FILLED HERE. IT SHALL BE FILLED AND UPLOADED IN THE PRICE BID OF E-PROCUREMENT PORTAL ONLY.	DETAILS NOT TO BE FILLED HERE. BIDDERS HAVE TO UPLOAD THE DULY FILLED TABLE 4.3.1 AND TABLE 4.3.2 ALONG WITH 'LETTER OF PRICE BID' AS PART OF FINANCIAL BID IN CPP E-PROCUREMENT PORTAL ONLY. STRICTLY IT SHOULD NOT BE UPLOADED AS PART OF TECHNICAL BID.
4	Part 3	Particular Conditions	52	“Payment of the amount due in: (A) local currency, payable from the proceeds of the Loan, shall be made through as stated in the Contract Data; and (B) foreign currency, payable from the proceeds of the Loan, shall be made through as stated in the Contract Data. Payment of the amount due in each currency, payable from any source of finance other than the Loan Agreement such as the Employer’s own funds, shall be made directly into the bank account opened by the Contractor in the name of JV as notified by the Contractor.	“Payment of the amount due in: (A) local currency, payable from the proceeds of the Loan, shall be made through as stated in the Contract Data; and (B) foreign currency, payable from the proceeds of the Loan, shall be made through as stated in the Contract Data. Payment of the amount due in each currency, payable from any source of finance other than the Loan Agreement such as the Employer’s own funds, shall be made directly into the bank account (s), nominated by the Contractor.

Addendum-03 CMRL/PHASE -II/SYS/CP22/ASA04/2021 01 March 2022					
SN	**Part**	**Section**	**Clause**	**Original Bid condition**	**Revised bid condition**
5	Part 2	GS-Appendix 10	22	Meeting rooms shall be fitted with flat screen 55in TVs suitable for projection and video conferencing.	All meeting rooms shall be fitted with flat screen 55in TVs suitable for projection and video conferencing.Each Office shall be provided with one meeting room with video conferencing facility (eg: Logitech Rally with desk mounted mic or equivalent) integrated to the TV and wired broadband connection for undertaking video conferencing using popular applications like MS Teams, Webex etc.
6	Part 2	Particular Specifications	14.5.1.3	The Contractor shall submit all new versions to the Employer/Engineer for review along with all support documentation at least 2 weeks prior to their installation.	The Contractor shall submit all new versions to the Employer/Engineer for review along with all support documentation at least 2 weeks prior to their installation. This shall include brief description of the changes made, test reports, including the automated regression test reports (to avoid new technical/functional issues) , list of compatible versions of other Interfacing sub-system softwares etc.
7	Part 2	GS-Appendix 19			Pls find the attached document on ISS & CYBER SECURITY TECHNICAL REQUIREMENTS, the new addition to the General Specifications, list of appendix.

CHENNAI METRO RAIL LIMITED

CHENNAI METRO RAIL PROJECT PHASE 2

TENDER No. CP22/ASA04

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

PART - 2

EMPLOYER'S REQUIREMENTS

SECTION VI A

GENERAL SPECIFICATIONS

APPENDIX-19

ISS & CYBER SECURITY TECHNICAL REQUIREMENTS

Jan 2022

APPENDIX – I

ISS & CYBER SECURITY TECHNICAL REQUIREMENTS

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 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.

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

1.3 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.

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

1.5 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.

1.6 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

2.1 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.

2.2 For the purpose of this document:

2.1.1 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.

2.1.2 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.

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

2.3 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.

2.4 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:

2.4.1 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.

2.4.2 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.

2.4.3 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.

2.5 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.

2.6 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.

2.7 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.

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

a) Authentication and identification

b) Authorization and access control

c) Network security

d) Data security

e) Security architecture

f) Security administration

g) Network devices

h) Server, host and end-point security

i) Application and database security

j) Audit and monitoring

k) System availability and continuity

l) 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
FIPS 140	U.S. Government Computer Security Standard for the Accreditation of Cryptographic Modules
NIST SP 800-82	Guide to Industrial Control Systems (ICS) Security
NIST 800-125	Guide to Security for Full Virtualization Technologies

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
ACN	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)
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

Acronym	Meaning
ECMP	Equal-Cost MultiPath
EDR	Endpoint Detection and Response
F&EN	Fire & Emergency Network
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
NIST	National Institute of Standards and Technology
NMS	Network Management System
NOC	Network Operation Center
OCC	Operation Control Center
OCN	Operational Communication Network
OTP	One Time Password
OWASP	Open Web Application Security Project

Acronym	Meaning
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
SOC	Security Operation Center (physical)
SQL	Structured Query Language
SRA	Secure Remote Access
SSH	Secure Shell
SSL	Secure Sockets Layer
SW	Software

Acronym	Meaning
TBS	Time Based System
TCC	Temporary Control Center
TCMS	Traffic Control Management System
TD	Train Detector
TLC	Traffic Light Controller
TLCN	Traffic Light Communication Network
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

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

a) SCN (Signalling Communication Network)
b) OCN (Operational Communication Network)
c) ACN (Administrative Communication Network)
d) F&EN (Fire and Emergency) Network
e) Traffic Light Communication Network (TLCN)

5.2 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.

5.3 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.

5.4 The Traffic management is composed of three (3) standalone networks physically and logically separated from the CBN:

a) TLC communication network.
b) TD communication network.
c) Traffic VSS / CCTV communication network.

6. General Requirements

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

6.2 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.

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

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

6.5 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.

6.6 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.

6.7 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.

6.8 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.

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

6.10 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.

6.11 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).

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

6.13 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).

6.14 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.

6.15 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.

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

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

6.18 Personal Firewalls shall be installed on Workstations.

6.19 Laptop disks shall be encrypted.

6.20 All servers and Workstations shall be hardened.

6.21 Equipment Power Supply

A. Power supply

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

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

iii. **Redundant power supplies shall be used as required.**

B. Power supply interruption & UPS (Uninterruptible Power Supply)

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

ii. **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

A. 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

A. **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.

B. **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.

C. 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.

D. 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.

E. 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

A. 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.

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

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

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

E. 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.

F. 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).

G. 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.

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

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

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

K. 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.

L. 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.

M. 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)

A. 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.

B. 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.

C. 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.

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

E. 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.

F. 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.

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

H. 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)

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

B. The ISS shall implement and deploy strong DLP technology products.

C. 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.

D. 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.

E. 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

F. 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)

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

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

C. Response and mitigate – response and mitigate security events.

D.

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

8.5 Information Security and Supply Chain Risk Management Requirements

A. 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.

B. 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.

C. 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.

D. 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).

E. 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 H below.

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

F. Installation, integration, testing and handover of systems

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

b. The procedures shall be developed, 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.

G. Concessionaire's Requirements by Systems and Activities

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

b. 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.

c. 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.

d. 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.

e. 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.

H. 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 b., 8.5.6.c. and 8.5.6.d shall apply.	The provisions of Section 8.5.6 e. 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 b., 8.5.6.c. and 8.5.6.d. shall apply.	The provisions of Section 8.5.6 e. above (Qualified Personnel) shall apply with respect to	Only Qualified Personnel operating on behalf of the Concessionaire shall be permitted access to

Sub-System	**Equipment and System Related Requirements**	**Personnel Related Requirements**	**Restricted Access / Additional Requirements**
		all personnel involved in the design, construction, testing, commissioning, operation and maintenance.	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 b., 8.5.6.c. and 8.5.6.d. shall apply.	The provisions of Section 8.5.6 e. 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 b., 8.5.6.c. and 8.5.6.d. shall apply; and b. The HMI and the PLCs supplied shall be manufactured (produced) by the same (single) manufacturer; and c. 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 8.5.6 e. 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 P-SCADA 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
F-SCADA	a. The provisions of Sections 8.5.6 b., 8.5.6.c. and 8.5.6.d shall apply.; and b. The HMI and the PLCs supplied shall be manufactured (produced) by the same (single) manufacturer; and c. 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 8.5.6 e. 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 b. and 8.5.6.c. 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 not less than	The provisions of Section 8.5.6 e. 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
	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 b., 8.5.6.c. and 8.5.6.d shall apply, with respect to all security systems equipment (edge devices), HW & SW components; and	The provisions of Section 8.5.6 e. 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.

I. 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.

J. 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

Figure 1 is an overview of the Metro System's logical architecture and information flow:

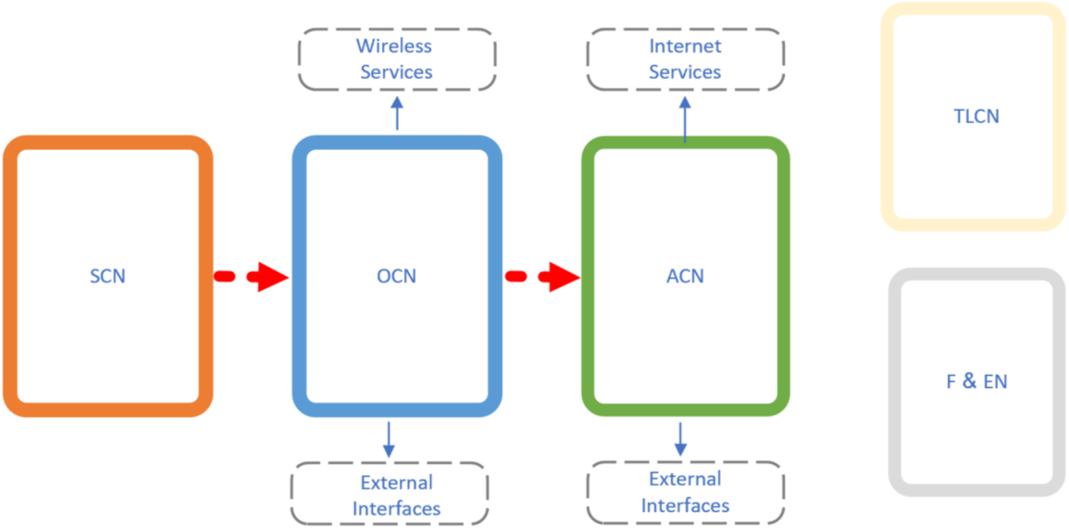

Figure 1: Logical Architecture and Information Flow (Conceptual)

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:

A. Impact on the public safety & human lives
B. Destruction or loss of critical services
C. Interruption of access to critical services, information or applications
D. Disclosure or viewing of critical or sensitive information
E. Modification of critical or sensitive information
F. 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:

A. Terrorists
B. Internal attackers
C. Disgruntled staff
D. Hackers
E. Criminals
F. Foreign intelligence services
G. Organized crime
H. Protesters and activists (e.g., environmental, political, animal rights)

9.4 Impacts

A. Safety, health and environmental event or damage to infrastructure: An event that results in harm to individuals, the environment or damage to the infrastructure.
B. 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.
C. 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.
D. 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.
E. Loss of business continuity.
F. 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

A. The system shall prevent simultaneous logins of a single user.

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

C. 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.

D. 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.

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

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

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

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

I. User authentication information shall not be exposed on any output.

J. 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

A. 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.

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

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

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

10.3 Authorization and Access Control

A. 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 physically separated through a guaranteed one-way traffic mechanism. Logical segmentation for each network shall segregate the internal networks.

c. 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.

d. 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.

e. Separation of development, test and production environments is required. Data transfer between environments shall be done in a controlled manner.

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

g. 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.

h. 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.

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

j. 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.**

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

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

m. 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.

n. 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.**

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

p. 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.

q. 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.

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

B. 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 OCN 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:

A. Firewall – Firewall devices capable of traffic stateful inspection and certified for ISO 15408 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.

B. 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.

C. 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.

D. 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.

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

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

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

H. 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.

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

J. 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.

K. 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.

L. 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.

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

N. 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.

O. 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.

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

Q. A structured Testing environment for updates is required.

10.5 Firewalls

Firewalls shall comply with the following:

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

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

C. Firewall Services shall follow industry best practices

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

E. 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

A. 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.

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

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

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

E. 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.

F. 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.

G. 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. The mediation process shall follow industry best practices.

10.7 Security Administration

A. Security policy and procedures

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

B. 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.

C. 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 OCN 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

A. 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.

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

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

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

10.9 Server, Host and End-point Security

A. 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, OCN, ACN, SCADA, TCMS and Rolling Stock On-board equipment as well.

B. 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.

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

D. 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.

E. 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.

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

G. 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).

H. 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

A. 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. **Applications providing web interfaces shall comply with current OWASP secure web development guidelines.**
- c. **Applications shall never connect to a database using the database administrator account or an account with system or management privileges.**
- d. **Generally accepted principles for secure coding (SDLC) shall be implemented for all applications development.**
- e. **Mobile code – process for authorization, monitoring, and control of the use of mobile code within the information system shall be established.**
- f. **Applications shall utilize prepared SQL statements and/or stored procedures to minimize the risk of SQL injection.**
- g. **All access to the database services shall be implemented using a dedicated Data Access Layer Component (DALC).**
- h. **Applications shall support updated encryption protocols, with 256-bit minimum, for all communications interfaces.**
- i. **The application shall validate all provided inputs and shall not trust submitted or presented data.**
- j. **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.**
- k. **Standard cryptographic APIs shall be used for cryptographic processing, if applicable (i.e., Bsafe, OpenSSL).**

B. 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/TCC 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)

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

D. 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.

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

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

G. 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.

H. 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.

I. 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.

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

K. 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.

L. 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

A. 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) capabilities as required in the Transit Management Systems document and systems specifications.

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

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

D. 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.

E. Each environment shall be individually backed-up.

F. Metro System security shall comply with RAM requirements.

10.12 Technological Means for Security

A. 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.

B. Refer to the Security Requirements of the Data Centers, as specified in the Transit Management Systems document .

C. 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, , as specified in the Transit Management Systems document and the Security Systems .

D. 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.

E. 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

A. 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.

B. 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:

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

B. 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.

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

D. User permission shall be based on RBAC mechanism.

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

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

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

H. 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.

I. The outgoing communications flow between the SCN and the OCN 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).

J. 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.

K. 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.

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

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

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

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

P. 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.

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

R. Unused network ports on devices and equipment shall be disabled.

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

T. All built-in system security features shall be enabled.

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

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

W. Hard drive locks shall be implemented.

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

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

11.2 OCN – Operational Communication Network

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

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

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

C. User permission shall be based on an RBAC mechanism.

D. Dedicated IT, Networking and security infrastructure shall be implemented.

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

F. OCN network traffic with ACN shall be controlled by security device. The traffic flows shall be permitted on a business needs basis only.

G. OCN core network stateful Firewall shall be implemented for networks segmentation.

H. 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.

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

J. 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.

K. Download and execution of unauthorized mobile code shall be blocked.

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

M. Unused network ports on devices and equipment shall be disabled.

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

O. All built-in system security features shall be enabled.

P. Hard drive locks shall be implemented.

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

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

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

T. All unnecessary ports and services in embedded devices such as PLCs and RIU's shall be disabled.

11.3 ACN – Administrative Communication Network

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

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

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

C. User permissions shall be based on an RBAC mechanism.

D. ACN 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.

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

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

G. Unused network ports on devices and equipment shall be disabled.

H. 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.

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

J. Hard drive locks shall be implemented.

K. 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.

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

11.4 F&EN (Fire and Emergency Network)

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

A. Strong authentication – such as token based, with PIN or smartcard, biometric and machine-based certificates.

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

C. User permission shall be based on an RBAC mechanism.

D. Dedicated IT, Networking and security infrastructure shall be implemented.

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

F. If needed, F&EN network traffic with the OCN shall be controlled by a security device. The traffic flows shall be permitted on a business needs basis only.

G. An F&EN core network stateful Firewall shall be implemented for networks segmentation.

H. Remote access implementation in this network shall be permitted only for compelling operational needs, shall be strictly controlled, and shall be preapproved 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.

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

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

K. Download and execution of unauthorized mobile code shall be blocked.

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

M. Unused network ports on devices and equipment shall be disabled.

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

O. All built-in system security features shall be enabled.

P. Hard drive locks shall be implemented.

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

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

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

T. All unnecessary ports and services in embedded devices such as PLCs and RIU's shall be disabled.

11.5 Traffic Light Communication Network (TLCN)

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

A. Strong authentication – such as token based with PIN or smartcard, biometric and machine-based certificates.

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

C. User permission shall be based on an RBAC mechanism.

D. Dedicated IT, Networking and security infrastructure shall be implemented.

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

F. TLCN network traffic with the OCN shall be controlled by a security device. The traffic flows shall be permitted on a business needs basis only.

G. A TLCN core network stateful Firewall shall be implemented for networks segmentation.

H. Remote access implementation in this network shall be permitted only for compelling operational needs, shall be strictly controlled, and shall be preapproved 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.

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

J. 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.

K. Download and execution of unauthorized mobile code shall be blocked.

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

M. Unused network ports on devices and equipment shall be disabled.

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

O. All built-in system security features shall be enabled.

P. Hard drive locks shall be implemented.

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

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

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

T. All unnecessary ports and services in embedded devices such as PLCs and RIU's shall be disabled.

12. Security Systems Specific Requirements

12.1 General

A. 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 (OCN).

   c. Administrative Communication Network (ACN).

B. 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)

A. The RSS resides in the ACN network, which is physically separated from the OCN and SCN networks.

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

C. 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.

D. 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

A. 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 OCN. The connection between these networks shall be protected in order to prevent unauthorized access to the networks.

B. 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.

C. The rolling stock systems which are related to the OCN network 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.

D. 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.

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

12.4 ATS and SCADA Interface

A. The ATS is physically separated from the Power SCADA.

B. 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.

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

D. 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)

A. 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.

B. 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.

C. 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.

D. 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 OCN FW.

c. An independent dedicated encrypted tunnel shall be established between the Cellular service provider's data network and the OCN. 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. A physically segregated Pre-production (Staging) environment shall be implemented.

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

C. 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.

D. 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.

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

13.2 Testbed and Model

A. 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.

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

C. 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.

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

E. 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.**

F. Test environment components shall include all systems and subsystems as detailed in the functional subsystems mapping (Appendix, section11).

G. Testbed complexes:

   a. **Test complex.**

   b. **Scenarios complex.**

   c. **Scenarios management complex.**

   d. **Testbed management complex.**

   e. **Debriefing complex.**

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

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

J. 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

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

B. 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.

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

D. 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.

E. 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)

A. 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.

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

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

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

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

F. 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.

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