ANNEXURE-'B'

SCOPE OF WORK

1.0 INTRODUCTION

LAN, Railnet & Internet System of RDSO is working with 150 Mbps link for LAN, 100 Mbps for IPDSLAM, 8 Mbps for DG office/house and 4 Mbps for IP video phone. All data exchanged over internet link is provided by M/s Railtel Corporation of India (RCIL). Two number of Web Servers having IP Address 10.100.2.19 and 10.100.2.12 for Railnet & Intranet respectively running on static IP web based application. Intranet server is visible in side RDSO & Railnet server is visible within Indian railways own netwok called Railnet.The cyber security of all data of intranet which are exchanged through internet web based application is very vital. Security audit of various network equipment & servers are to be carried as per scope of works given in para 2.0 & 3.0 by the third party CERT-In Empanelled Auditors. The details of equipment i.e. Firewall, Core Switch, Distribution switch and L3, L2 managed switch are given Para 5.0. Work would be carried out in 2 phases, details of which are as under.

2.0 Phase - I

2.1 Audit of internet links operating through firewall, core switches, distribution switch and server for vulnerability Assessment (VA), Penetration Testing (PT), Web Application Security Assessment (WASA) which would include the following.

2.1.1 Classification of web internet links security in firewall in terms of sensitivity and level of access.
2.1.2 Personnel data access control matrix based on the above classification.
2.1.3 Secured database configuration parameters.
2.1.4 Password complexity and authentication mechanism.
2.1.5 Privilege given on above objects as per above access control matrix.
2.1.6 Criticality and protection of test data and information.
2.1.7 Data backup mechanism and procedures

2.2 Audit of Operating Systems for vulnerability Assessment (VA), Penetration Testing (PT), Web Application Security Assessment (WASA) which include the following.

2.2.1 Secured OS installation on Window Servers.
2.2.2 Patch and service pack levels for the OS as applicable.
2.2.3 User's group creation, user management and password complexity.
2.2.4 File system security of the OS.
2.2.5 Access rights and privileges.
2.2.6 Services and ports accessible.
2.2.7 Change management in term of modification to the OS.
2.2.8 Backup and emergency response measures.
2.2.9 Determine antivirus configuration ,architecture ,definition, dates, scanning and updating policies
2.2.10 Create baseline of critical parameters of the servers and OS configuration.

2.3 Audit of Switches for vulnerability Assessment (VA), Penetration Testing (PT), Web Application Security Assessment (WASA) which include the following.

2.3.1 Latest IOS.

This PDF file is created with a trial version of RealPDF. To remove this mark, buy the full version.

2.3.2 Check of configuration access.
2.3.3 Verify access Control list.
2.3.4 Check for unnecessary services.
2.3.5 Check for unnecessary protocols.
2.3.6 Audit logs.
2.3.7 Log functions.

2.4 Audit of Server Ports:
2.4.1 Weak passwords.
2.4.2 Un-patched software.
2.4.3 Unnecessary services running.
2.4.4 Mis-configuration.

2.5 Audit of Web Application for vulnerability Assessment (VA), Penetration Testing (PT), Web Application Security Assessment (WASA) which include the following.

2.5.1 Audit of web application and its associated application should be carried out on the basis of the most dangerous web application security flaws along with effective methods of dealing with those flaws as under.

A1- Injection
A2- Broken authentication and session management
A3- Cross Site scripting (XSS)
A4- Insecure direct Object References
A5- Security Mis-configuration
A6- Sensitive data exposure
A7- Missing Function level Access Control
A8- Cross-Site Request Forgery
A9- Using known Vulnerable Components
A10- Un-validated Redirects and forwards

3.0 Phase-II

3.1 The follow-up audit to check the status of rectification of observation mentioned in the Phase is to be carried out.
3.2 RDSO would initiate the rectification of the observations as mentioned in Phase - I audit reports.
3.3 In Phase-II, the auditor needs to check the status of the rectification done with respect to observations given in the Phase-I.
3.4 Final the auditor to submit the final audit certificate.

4.0 Deliverables:

4.1 At the end of Phase -I:
4.1.1 A draft audit report after phase-I for comments by RDSO.
4.1.2 Executive summary for the observations with recommendations.

4.2 At the end of Phase II:
4.2.1 Final audit report after rectification are carried out by RDSO administration.
4.2.2 Issue of audit certificate

This PDF file is created with a trial version of RealPDF. To remove this mark, buy the full version.

5.0 Detail of equipments connected in network of RDSO.

Sr. No.	Description of item	Unit	Qty.
1	**Core Switch (Cisco WS-C 6509E)** (i) Supervisory Engine Redundant {Module VS SUP-2 T-10G (CPU)*2 nos. with 10G Fiber modules-4 nos.} ii)Power Supply Redundant-2 nos. iii) Fibre Ports 1G- 48 nos. {Module WS-X6824- SFP, 24Ports*2nos.}with 24 nos. LX Fiber modules compatible with Single Mode OFC. iv) Fibre Port 10G - 4 nos.{Module WS-X6704-10GE,4 Port } with 10G Fiber modules.. v)Ethernet Port RJ45-48 nos.{Module WSX 6848-GE-TX} with FAN Module	Nos.	2
2	**Distribution Switch (Cisco 4503e)** (i) Supervisory Engine {Module WS-X45-SUP 7LE with 4 fiber ports (1G/10G)} (ii) Power Supply Redundant -2 nos. module with FAN Module (iii) Ethernet Port -48 Nos.	Nos.	3
3	**Firewall (Cisco - ASA 5525x)** Mgt Port: 1, LAN Port: 8, USB Port:2	Nos.	1
4	**Router (CISCO 2800 Series)** Console Port: 1 AUX Port: 1, LAN Port: 2, Serial Port: 4	Nos.	1
5	**L3 Managed Switch (Cisco 3750)** Ethernet Port RJ45- 24 nos., Fibre Port 1G- 4 nos.	Nos.	22
6	**Server (HP Prolient DL 380 G5)** Processor: Intel Xeon X 2, 2.0 GHz RAM: 2GB , HDD: 146GB X 4., OS: Windows 2003 server,64 Bit	Nos.	1
7	**Server (HP Prolient DL 380 G4)** Processor: Intel Xeon X 2, 3.4 GHz RAM: 1GB, HDD: 72.8GB X 3, OS: Windows 2003 server, 64 Bit	Nos.	1
8	**L2 Managed Switch (Cisco 2960)** Ethernet Port RJ45- 24 nos., Fibre Port 1G- 4 nos.	Nos.	50
9	**L2 Managed Switch (Extreme Summit x450e-24p)** Ethernet Port RJ45- 24 nos., Fibre Port 1G- 4 nos.	Nos.	11
10	**L2 PoE Switch (Extreme Summit 200)** Ethernet Port RJ45- 8 nos., Fibre Port 1G- 2 nos.	Nos.	7
11	**L2** Managed **Switch (HP Procurve)** Ethernet Port RJ45- 24 nos. , Fibre Port 1G- 4 nos.	Nos.	1
12	**L2 Managed Switch (Cisco Linksys)** Ethernet Port RJ45- 24 nos. Fibre Port 1G- 4 nos.	Nos.	4
13	**L2 Managed Switch (D-Link- DES 1024R,DGS-3200-24 or similar)** Ethernet Port RJ45- 24 nos. , Fibre Port 1G- 4 nos.	Nos.	10
14	**L2 Switch (D Link)** Ethernet Port RJ45- 24 nos.	Nos.	2

(A.K.Jayaswal)
Assistant Design Engineer /TMS
For and on behalf of President of India

This PDF file is created with a trial version of RealPDF. To remove this mark, buy the full version.