



SECURITIES AND EXCHANGE BOARD OF INDIA
Integrated Surveillance Department
SEBI Bhavan 5th Floor A Wing
C-4 A G Block, Bandra Kurla Complex
Bandra (E) Mumbai
Tel: 26449000
Fax: 26449024

REQUEST FOR PROPOSAL
For
Design, Supply,
Installation, Configuration, Operationalization and
Maintenance of IT Infrastructure for
IMSS project

TENDER NOTICE NO. : **SEBI/IMSS/2011/01**

DATE OF ISSUE: August 02, 2011

DUE DATE: September 09, 2011 before 03:00 P.M.

NAME & ADDRESS OF CLIENT: Officer on Special Duty
Securities and Exchange Board of India
Fifth Floor, SEBI Bhavan "A" Wing,
Bandra Kurla Complex Bandra (East) - 400 051
India.
Fax: 26449024



**SECURITIES AND EXCHANGE BOARD OF INDIA,
MUMBAI**

REQUEST FOR PROPOSAL

FOR

**Design, Supply,
Installation, Configuration, Operationalization and
Maintenance of IT Infrastructure for
IMSS project**

INTEGRATED MARKET SURVEILLANCE SYSTEM

TABLE OF CONTENTS

SECTION 1	5
1.1 OBJECTIVE	5
1.2 OVERVIEW	5
1.3 ELIGIBILITY CRITERIA	6
1.4 BIDDING PROCESS	7
SECTION 2	9
TECHNICAL REQUIREMENTS FOR IMSS IT UPGRADE.....	9
2.1 PROPOSED ARCHITECTURE FOR IT INFRASTRUCTURE SETUP FOR IMSS	9
2.2 ESTIMATE OF EQUIPMENTS	10
2.3 CURRENT IMSS-IT INFRASTRUCTURE SETUP	10
2.4 AMC FOR EXITING PRODUCTION SERVERS.....	11
2.5 BUYBACK OF ITEMS IN EXISTING SETUP.....	11
2.6 IMPLEMENTATION METHODOLOGY	12
I. HARDWARE/ SIZING/ PERFORMANCE REQUIREMENTS:	12
II. UPGRADE/ INSTALLATION TASKS.....	13
III. FUNCTIONALITY OF THE SYSTEMS COMPONENTS.....	17
SECTION 3	19
WARRANTY AND SUPPORT	19
3.1 SUPPORT	19
3.2 WARRANTY	20
3.3 COMPLIANCE TO SPECIFICATIONS	22
3.4 MAINTENANCE	22
SECTION 4	25
4.1 BIDDERS RESPONSE SHEET	25
SECTION 5	33
COMMERCIAL TERMS AND CONDITIONS.....	33
5.1 GENERAL TERMS AND CONDITIONS.....	33
5.2 RIGHTS OF SEBI.....	34
5.3 CLARIFICATION ON RFP	35
5.4 PRICES	36
5.5 PAYMENT TERMS	36
5.6 PERFORMANCE BANK GUARANTEE	37
5.6 DELAYS IN THE VENDOR'S PERFORMANCE	37
5.7 DELIVERY, INSTALLATION AND COMMISSIONING.....	38

5.8	INSURANCE.....	39
5.9	SUBMISSION OF BIDS	39
	<i>SECTION 6</i>	41
	ANNEXURES	41
	ANNEXURE A.....	41
	BENCHMARKING FOR PERFORMANCE	41
	ANNEXURE B	42
	PROPOSED TECHNICAL SPECIFICATIONS.....	42
	ANNEXURE C	56
	ANNEXURE D.....	68
	IMSS WAN CONNECTIVITY DIAGRAM.....	68
	NETWORK ARCHITECTURE	69
	ANNEXURE E	70
	PERFORMANCE BANK GUARANTEE.....	70
	ANNEXURE F	73
	TENDER FORM-TECHNICAL BID	73
	ANNEXURE G.....	75
	TENDER FORM-COMMERCIAL BID	75
	ANNEXURE H.....	78
	BILL OF MATERIALS - IT INFRASTRUCTURE UPGRADE.....	78
	ANNEXURE I - (CHECKLIST)	81

SECTION 1

1.1 Objective

Upgrade of IT infrastructure of Integrated Market Surveillance System (IMSS) installed at data centre, Mumbai; DR site, Chennai and Data sources (NSE, BSE, NSDL, CDSL and MCX). The scope of work comprises of design, supply, installation, configuration, operationalization and maintenance of IT Infrastructure.

1.2 Overview

Brief summary of Integrated Market Surveillance system (IMSS)

The Integrated Market Surveillance System (IMSS) used for Market Surveillance was put on use from December 2006. The system collects transaction and master data from exchanges (NSE, BSE, and MCX) and depositories (NSDL, CDSL) on a daily basis to generate alerts for predefined market manipulation scenarios. It also provides powerful data analysis and benchmarking tools.

Main components of IMSS are:

Application Software:

SMARTS surveillance application software used for generation of alerts and analysis of data. This comprises of

- a. Custom developed conversion programs for Extraction, Transformation and Loading of data into the system
- b. Off-the-shelf SMARTS data analysis, alert generating and reporting tools
- c. Custom developed alert generation programs

IT infrastructure:

- a. Servers and storage for data processing and storage
- b. Network and security infrastructure for collection of data
- c. Ancillary systems for support and daily operations

Technical support services:

- a. Daily operational support for data collection and processing
- b. Network and Security Monitoring services through operation centers
- c. Warranty and maintenance services

1.3 Eligibility Criteria

The Bidders must meet the following eligibility criteria

- i. The bidder should have the ability to supply, install, design & implement and maintain the required hardware/ operating system, application software (like security application, databases etc.) and utilities.
- ii. The bidder must have a System Integrator (SI) expertise in the implementation of end to end solution architecture in the area of proposed upgrade. "Bidder" is either an entity or the lead bidder of a consortium (where more than one entity have partnered), which exhibits its interest in response.
- iii. The bidder should have successfully implemented similar kind of project or upgrade in the financial sector, preferably with the proposed solution in a Stock Exchange/Regulatory Authority in India or internationally. The bidder should submit
 - A write up on company's experience as a provider of a solution for establishing a similar kind of undertaking.
 - List of current/recent clients/references (related with aforesaid requirement) wherein project/upgrade completed entails handling similar complexity and data size.
- iv. The bidder should have Technical support office at Mumbai and Chennai. The bidder must have proven financial and Organizational strength to undertake and execute the project. The annual turnover of bidding company (not parent company) for the last three Commercial years should be not less than Thousand Crores. Proof of the financial turnover or audited financial statements for the past three years should be submitted along with the proposal.
- v. Bidder must have ISO 9001 certification or above.
- vi. The bidder should have valid authorization from and active relationship with Software owners (Off-the-Shelf Software or any other software which are proposed as part of the upgrade) or Hardware manufacturers for a minimum period of one year prior to the date of release of this RFP.
- vii. Bidder must provide evidence that it is a current legal entity and must warrant that it is financially solvent i.e. it is able to meet all its debt as and when due.
- viii. Bidder must submit a detailed statement of facts and profile of company including year of commencement of business, Internet site details, name and title of the authorized signatory for their Bid, their contact numbers and e-mail address.

- ix. Bidder must warrant that no legal action is pending against them for any cause in any legal jurisdiction. If such actions are pending, the Bidder must provide details of such action (s) and explain as to how such pending action does not affect its ability to deliver the RFP requirements.
- x. These eligibility criteria are neither exhaustive nor in any particular order of significance. Any bid not meeting all of these minimum eligibility criteria is liable to be rejected by SEBI.

1.4 Bidding Process

Bidders shall submit their Bids in two separate parts as follows:

- i. Technical Bid containing the exhaustive and comprehensive Technical solution details and;
- ii. Commercial Bid containing the pricing information.

The Technical Bids should NOT contain any pricing or commercial information. However, a masked bill of materials masking the price information should be provided along with the technical bid.

Proposal Evaluation

Initially technical bids will be opened and evaluated. Those bidders who satisfy the technical requirements of the solution as per the requirements/specifications and the terms and conditions of this document, shall be short-listed. Commercial bids shall be opened only for the short-listed bidders who have qualified in the technical bid.

Technical Evaluation

The proposals will be technically evaluated using a scoring process based on various components. Each response to the RFP from each bidder will be judged and scored on its own merit.

As part of the technical bid evaluation, bidders will be required to demonstrate to SEBI and its technical committee, their existing project or upgrade of similar nature, which forms part of the knowledge base of the bidder for providing solution to SEBI.

The scoring process will be based broadly on the following main components

- Bidder capability including proven relevant experience –25 %
- Core systems – Production servers – POC - 25 %

- Understanding of SEBI's requirement and proposed Solution Architecture (Hardware,Software,Network and Security etc) – 50 %

The bidders scoring above 65% in each of the 3 components and 75% overall will only be technically qualified and top three of these will only be short listed and considered for commercial evaluation.

As part of the evaluation process, the short listed bidders may be required to demonstrate Proof of Concept (POC) based on existing sample data for core systems. Benchmarking testing should be carried out by bidder in conjunction with SEBI officials as part of the POC. Estimated time required for this exercise should not exceed more than 4 working days. The details of benchmarking task for measuring performance of the system are enclosed at "**Annexure A**".

Commercial Evaluation

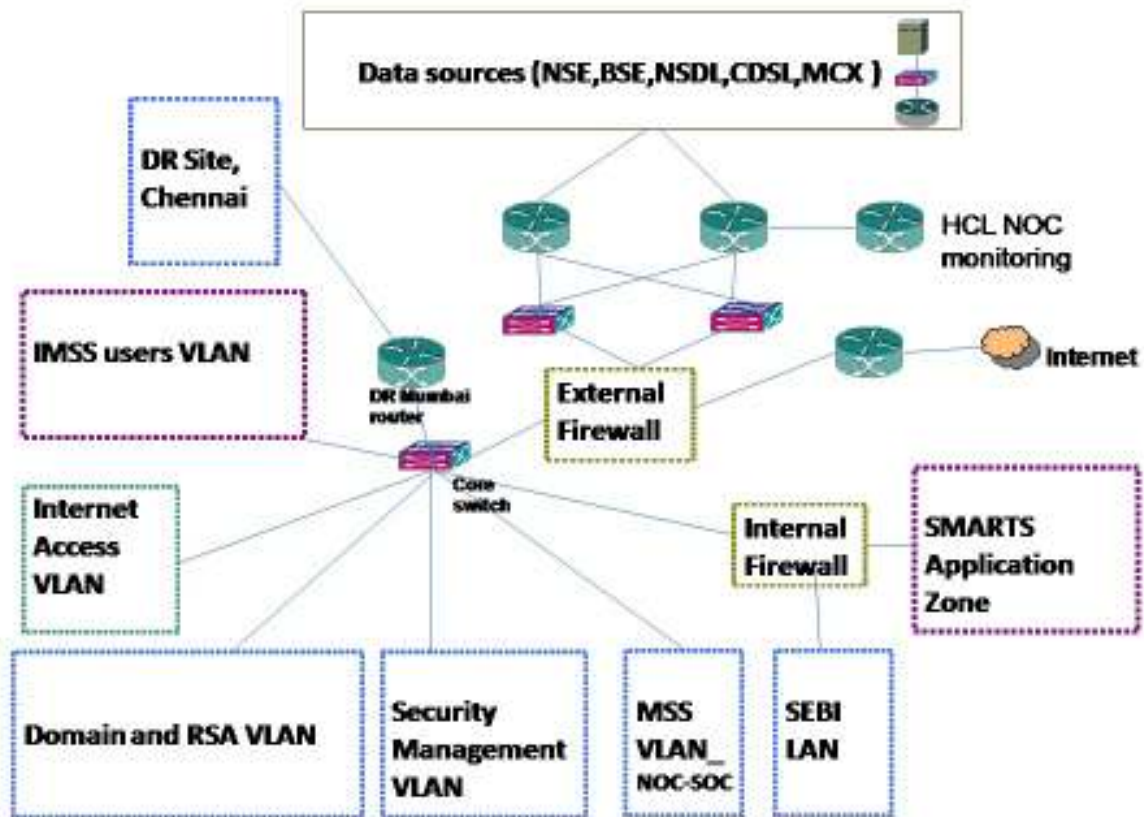
The commercial bids of the short listed bidders will be evaluated on the basis of Total Cost of Ownership (TCO) over a six year period converted to Net Present Value(NPV) calculated using a nominal interest rate of 8% per annum for second and subsequent years of the duration. The bidder with the lowest NPV, termed L1 bidder, shall qualify for further negotiations and award of contract.

SECTION 2

TECHNICAL REQUIREMENTS FOR IMSS IT UPGRADE

2.1 Proposed Architecture for IT infrastructure setup for IMSS

Indicative system architecture of proposed solution for upgrade is given below. However, if the bidder has a better and more elegant "Architecture" he/she is free to propose the same.



2.2 Estimate of equipments

An indicative list of the equipments required for the proposed infrastructure upgrade is given below. Bidders are required to find out actual numbers of equipments as per their proposal. The specifications of the proposed items are placed at “Annexure ‘B’”.

Location: IMSS Data Centre, Mumbai

S/N	Items/Hardware	Estimated Qty
1	Production servers	5
2	Support Servers	8
3	Cisco Routers	4
4	Cisco Switches	10
5	Firewalls	4
6	IDS/IPS	2
7	Storage system	1
8	SAN Switch	2

Location: IMSS DR site Centre, Chennai

S/N	Items/Hardware	Estimated Qty
1	Production servers	1
2	Support Servers	8
3	Cisco Routers	2
4	Cisco Switches	6
5	Firewalls	2
6	IDS/IPS	1
7	Backup device	1
8	SAN Switch	1

Location: Data sources (NSE, BSE, NSDL, CDSL, and MCX)

S/N	Items/Hardware	Estimated Qty
1	Servers	2 x 5
2	Routers	1 x 5
3	Switches	2 x 5

**One server, switch and router is installed at each of the data sources currently.*

2.3 Current IMSS-IT Infrastructure Setup

- i. The Existing network and communication backbone of SEBI-IMSS along with network architecture is placed at “Annexure D “

- ii. Specifications of current IT infrastructure of IMSS are given in “**Annexure C**”. It provides information about configuration/specifications and numbers of existing servers, network and security equipments at each location. Information about applications/software/utilities installed with the functionality of each of them are also been provided.

2.4 AMC for exiting production servers

Details of production servers and storage systems deployed at IMSS data centers are as under

S/N	Items	Qty	Location	AMC till date
1	Sun Fire X4140	2	Data centre, Mumbai	10/10/2011
2	Sun Fire X4600	2		
3	Sun Storage ST6140A	1		25/02/2012
4	SunFire V490	2		
5	StoreEdge 3510	1		
6	Sun Fire X4140	1	DR site, Chennai	10/10/2011
7	Sun Fire X4600	1		
8	Sun Fire V240	2		25/02/2012
9	StoreEdge 3510	1		

SEBI is planning to keep some of the Production servers and all storage systems deployed in current IMSS setup. The bidder should provide AMC for these equipments as part of the upgrade. Bidder should quote for AMC renewal of these equipments separately in the bill of materials. From the above list, item nos 4 and 8 (SunFire V490 and SunFire V240 servers) need to be replaced with the required numbers of proposed production servers.

2.5 Buyback of items in existing setup

The bidder should offer buyback of existing equipments which will be replaced by the new items. The details of equipments are placed in **Annexure C**.

Bidder shall furnish Buyback price in the following format:

S/N	Items/hardware	Qty	Unit Price	Total(Rs.)
1	Servers			
2	Cisco Routers			
3	Cisco Switches			
4	Firewalls			
5	IDS			
6	Any other			

2.6 Implementation Methodology

i. Hardware/ Sizing/ Performance Requirements:

The bidder must specify the entire bill of materials including hardware, network and security equipments, software. The bidder must size the components of the proposed solution to meet the throughput, capacity and performance. The bidder shall submit the sizing methodology in response to the RFP. Bidder must configure the solution architecture in such a way that it does not have any single point of failure. Adequate on site spares or availability of such spares within the specified time frame of uptime requirements to restore the system back to normal state in the event of failure should be provided. The bidder must clearly propose and specify applications/software/utilities compatible with existing application/utilities installed mentioned in “**Annexure C**”. The bidder is responsible for supply, installation; configuration of entire solution ensuring existing functionality will be maintained.

The proposed upgrade solution architecture should be able to handle huge amount of data transfer and processing.

- a) Data acquisition setup should be able to collect 200-300GB of raw data daily. This data will be available for acquisition by 2100 hrs every day. The bidder should ensure that the proposed system has the capacity for collecting, transforming, loading and processing the aforesaid size of data by 0800 hrs on the next day using the existing software programs..
- b) Proposed data storage should be able to expand up to 200 TB.
- c) Availability of system
 - High availability / cluster solution with minimum 98.5% uptime for all critical servers/network and security equipments.
 - Maximum permissible down time of the system in any single event is 8 hours.
 - Uptime percentage shall be calculated as (100 – downtime percentage). Downtime percentage shall be calculated as unavailable time divided by total available time, calculated on a half yearly basis. Total available time is for 5 (five) days a week, between 0800 hrs to 2000 hours. Unavailable Time is time involved while any part of the core configuration or system software component is inoperative. The process of applying upgrades, updates and patches shall not affect system uptime.
- d) Concurrent users
The number of full time users is currently 25 but the same will be doubled within timeframe of 5 years. There will be other users also accessing the system in a limited way. The system should support additional 30 users with limited access provisions. These users will be part time users to support investigations, inspections etc.
- e) Scalable and upgradeable architecture

SEBI envisages in-box scalability with the provision to enhance the capacity of the proposed system on demand. The system must also be scalable to acquire and process data on-line/real-time basis.

It is to be noted that the configuration proposed by the bidder should completely meet all the stated requirements and in addition should be field upgradeable to handle the future requirements extending to twice the current load with the same level of performance.

- f) Bidder must ensure that all the functionality currently available in existing IMSS IT Infrastructure setup should be maintained in the proposed solution architecture as well.

ii. Upgrade/ Installation Tasks

Identified installation/upgrade tasks envisaged to be done by the bidder and that of existing solution partner of IMSS (M/s HCL Technologies Ltd) are given below. To ensure a smooth and seamless upgrade and integration, both the parties should work jointly to handle the work wherever necessary.

S/N	Items	Tasks	
		Vendor tasks	HCL tasks
1	Production servers at data centre, Mumbai.	Server installation #	SMARTS software installation, data extraction, conversion programs installation, compilation and verification, installation of programs for alert generation, crontab scheduling, configuration restoration etc.
2	Storage at data centre, Mumbai	Installation, partitioning and initial configuration	Integration with existing storage
3	Support servers at data centre, Mumbai	Server installation # Installation of respective applications /software to ensure existing functionality of servers would be maintained: List of existing applications/ software/ utilities or any other compatible applications /software /utilities to be installed and configured on respective servers: 1. Trend Micro Antivirus 2. Interscan message security suite 3. Interscan web security suite 4. Web sense enterprise	HCL will provide adequate support to the vendor for restoration configuration of rules and policies of existing setup on the upgraded setup

		<p>manager</p> <ol style="list-style-type: none"> 5. Web trend firewall suite 6. Cisco ADSM utility 7. Squid 8. ISS site protector 9. Checkpoint SMARTS dashboard 10. RSA ACE server <p>Policies as configured on existing setup needs to be installed and configured.</p>	
4	Servers at data sources (NSE, BSE, NSDL, CDSL, MCX)	Server installation #	Restore data transfer scripts if any, restore existing directory structure at data sources
5	Network installation at data centre, Mumbai	<p>Routers - installation and initial configuration</p> <p>Restore configuration of existing primary and backup router, ACL configuration, Leased lines and PRI configuration, NOC/SOC configuration (NISP&SISP rules and policies) ##.</p>	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
		<p>Switches - installation and initial configuration.</p> <p>Restore core switch configuration, VLANs configuration, ACL rules and policies installation (NISP&SISP rules and policies) ##.</p>	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
6	Security installation at data centre, Mumbai	<p>Firewall - installation and initial configuration.</p> <p>Restore configuration of security devices , ACL, policies, monitoring scripts, firewall rule base to policy mapping on respective servers, etc.</p>	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.

		IDS - installation and initial configuration. IDS configurations, NISP&SISP rules and policies implementation. ##	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
7	Network installation at data sources (NSE, BSE, NSDL, CDSL, MCX)	Routers - installations and initial configuration. Restore configuration of routers, ACL, policies (NISP&SISP rules and policies) ##	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
		Switches - installations and initial configuration Existing switch configuration, VLANs configuration, ACL rules and policies implementation (NISP&SISP rules and policies) ##	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
8	Production Servers at DR site, Chennai	Server installation #	SMARTS software installation, data extraction, conversion programs installation, compilation and verification, installation of programs for alert generation, crontab scheduling, configuration restoration etc.
9	Support server at DR Site, Chennai	Server installation # Installation of respective applications /software to ensure existing functionality of servers would be maintained: List of existing applications/ software/ utilities or any other compatible applications /software /utilities to be installed and configured on respective servers: 1. Trend Micro Antivirus 2. Interscan message security suite 3. Interscan web security suite	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.

		<p>4. Web sense enterprise manager 5. Web trend firewall suite 6. Cisco ADSM utility 7. Squid 8. ISS site protector 9. Checkpoint SMARTS dashboard 10. RSA ACE server</p> <p>Policies as configured on existing setup needs to be installed and configured.</p>	
10	Network installation at DR Site, Chennai	<p>Routers - installations and initial configuration</p> <p>Restore configuration of existing primary and backup router, ACL configuration, Leased lines, PRI configuration, NOC/SOC configuration, NISP&SISP rules and policies implementation ##</p>	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
		<p>Switches - installations and initial configuration</p> <p>Restore core switch configuration, VLANs configuration, ACL, rules and policies installation ((NISP&SISP rules and policies).##</p>	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
11	Security installation at DR Site, Chennai	<p>Firewall</p> <p>Restore configuration of security devices, ACL, policies, monitoring scripts, firewall rule base to policy mapping on respective servers, etc</p>	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
		<p>IDS - installation and initial configuration.</p> <p>IDS configurations, NISP&SISP rules and policies implementation. ##</p>	HCL will provide adequate support to the vendor for restoration and configuration of rules and policies of existing setup on the upgraded setup.
12	Backup device at DR site	Installation and initial configuration	Implementation and configuration of backup policy

13	Daily application and network support	----	HCL onsite engineers, Workflow tasks defined
14	Backup of complete new setup	Installation and configuration	Backup based on configured backup policy
15	NOC/SOC support to monitor network and security devices	----	HCL NOC-SOC will provide 24 x 7 support.
16	SAN Switch	Installation and configuration	HCL will provide adequate support to the vendor

Note:

#: Server installation will include following but not limited to:

- OS installation,
- OS Hardening
- Upgrade, update, bug fixes, patches installation
- Clustering wherever applicable

NISP – Network Implementation and Support Plan

SISP – Security Implementation and Support Plan

iii. Functionality of the Systems Components

The bidder shall clearly specify the functionality of the components and accordingly provide the specifications of each of the delivered equipments. Bidder shall ensure that proposed system software/applications/utilities should be installed and configured to meet the existing functionality requirements.

The inputs given below will enable the bidders to arrive at solution architecture to meet the IT infrastructure requirement in detail.

- a. Currently IMSS is implemented on separate secured LAN. The data centre is connected to the data sources through leased terrestrial line as the primary connectivity and ISDN connectivity as a backup connectivity. Bidder shall be responsible for termination, testing and stabilization of leased lines and ISDN lines used for IMSS on new setup.
- b. The data transfer for all the confidential data from the external entities will be encrypted using IPsec 3DES. The routers and other networking equipment have to be configured to ensure that this requirement does not degrade the performance.

- c. Based on the above information, the bidder is expected to provide a comprehensive document giving details of the design, architecture, sizing of the equipments and bill of materials. Format of bill of materials is placed at **Annexure 'H'**.
- d. Apart from the encryption at the link level, the proposed solution by the bidder should include firewall and IDS/IPS (NIDS and HIDS) to provide a secure environment and also ensure that the network is free from the virus attacks, flooding, broadcast storms, DOS etc. as per the guidelines of CERT-IN.
- e. Bidder shall clearly mention EOL/EOSL period for each of the component in IT infrastructure setup. Bidder shall ensure that products quoted should be in current line of production and has maturity period of maximum six years from the date of installation. Bidders also should clearly define scope of replacement/support of EOL (End of Life) equipments in future.

SECTION 3

Warranty and Support

3.1 Support

The bidder must demonstrate capability to provide a superior standard of ongoing product support.

Bidder's response should identify for a projected 3 year post warranty support Go-Live.

- the location from which support is provided
- how support is to be provided (on-site, call basis, telephone, fax, e-mail etc)
- number and skill levels of support staff
- tools used to record and monitor support calls
- the problem escalation process for unresolved cases
- ability to provide support for problem diagnosis and rectification
- the standard service levels for support provided
- committed response times from call-out, to expert-on-site and commitments for time-to rectify

In case of consortium it is essential that one of the Indian partners well adequately trained to handle the software development activities.

Performance Monitoring & Tuning Tools

Currently, security and network monitoring is carried out through HCL's Security and Network Operation Centre. SEBI would like to retain their services. However, the bidder's response must describe the performance monitoring tools that will be provided along with the solution for the supplied products. These tools would be expected to provide current and historical information on system availability, response times and average and peak utilisation of system resources. Performance monitoring & tuning tools should also be capable of configuring supplied resources like hardware, system software, databases, etc. for optimum performance.

The bidder's response should describe what alerts are provided in the performance monitoring tools, e.g. potential software errors, threshold settings, process bottlenecks, critical events.

Upgrading System Components

The bidder's response should describe the processes that support the updating of system components, parameters and the impact of such updating on system availability.

3.2 Warranty

The Supplier represents and warrants that:

- (1) The Services and the Systems, Products or any software provided, do not infringe, and shall not infringe or cause the infringement of, the proprietary rights of any third party.
- (2) The Service and the System shall utilize current and proven technologies.
- (3) The Services to be provided hereunder shall be performed with qualified personnel in accordance with the applicable time schedules (or otherwise in a timely manner)
- (4) The Services and Systems shall be provided in a good and workmanlike manner, in accordance with the applicable Technical Specifications and Acceptance Criteria and at least at the same level and with the same degree of accuracy, quality, completeness, responsiveness and cost effectiveness which are consistent with good industry standards.
- (5) The Systems, Products or software provided hereunder properly interface with other systems, properly interface with each other, perform together as an integrated system and, as an integrated system, meet the warranties in the Contract, including but not limited to the meeting of the Technical Specifications.
- (6) The Systems provided hereunder shall function as designed and be fit for the purpose for which they have been provided and will be otherwise be free of errors and defects that interrupt systems operations or otherwise negatively impact normal operations or business processes.
- (7) During the term of this Contract, the Services, Systems and any software provided shall not contain or introduce any viruses, bugs or disabling Codes. In the event of any such virus being introduced into SEBI's systems, the Supplier shall use its best efforts to minimize the impact of such virus.

All the Hardware and Software supplied under the Contract should be covered under Warranty for the duration of the thirty-six months commencing from the date of acceptance of the total solution. This Warranty shall consist of the following:

- The correction of any defects that may arise from the design or workmanship or from any act or omission of the Supplier that may develop under normal use of the supplied Systems. Normal operating environmental conditions shall be specified in the Contract. On receiving the notification from SEBI, the Supplier should carry out the repair / replace the defective systems within a reasonable period of time. This reasonable period of time will be decided by SEBI at the time of entering into a

Contract with the successful bidder. This will be done at no extra cost to SEBI. Failure to remedy the defects within the period specified in the Contract, may involve remedial action by SEBI at the Suppliers' risk and expense and without prejudice to any rights that SEBI may have against the Supplier under the Contract.

- The provision of Application Maintenance Support including investigating and resolving technical and business problems relating to the IMSS due to the upgraded items, responding to user and SEBI's help requests that relate to IMSS IT infrastructure components, monitoring and advising SEBI on the near, medium and long term upgrade schedule for third party software that forms part of upgraded solution, installation of such upgrades, undertaking productivity improvements that will improve the service levels, assist in prioritizing the help requests and open problem tickets, resolving open problem tickets in accordance with their priority and regular updating of the documentation that relates to the IMSS IT infrastructure.
- The provision of Emergency Maintenance Support including providing support and remedial services for problems that render the IMSS unavailable or unresponsive; resolving any ABENDS and correcting errors or invalid data within the IMSS irrespective of the source of such problem; and working closely with SEBI to provide timely problem resolution and contingency planning for the IMSS.
- Corrective maintenance
- Preventive maintenance
- Enhancement Services: The Supplier shall provide ___ Man Months of Enhancement Services per calendar quarter or part thereof (Included Enhancement Effort) as part of the Warranty Services at no additional charge to SEBI. Supplier shall be responsible for collation of all enhancement requests submitted by the IMSS users and SEBI. The process for entering an enhancement request shall be agreed and set out in the contract. Supplier shall provide SEBI with an estimate of the effort necessary for the implementation of the requested enhancements. In the event that the effort required for implementation of the requested enhancements exceeds the available Included Enhancement Effort, Supplier shall, in consultation with SEBI and subject to SEBI approval, prioritize delivery of the enhancement services and implement them in a controlled and efficient fashion. Any enhancement effort in addition to the Included Enhancement Effort shall be provided on a time and materials basis at the rates agreed by the Parties in this regard and set forth in the Contract. Included Enhancement Effort that is not utilized in a calendar quarter shall be carried forward to the following quarters provided that such effort shall not carry over for more than three consecutive calendar quarters following the quarter in which such Included Enhancement Effort was originally available. Supplier shall work with SEBI to package maintenance patches and enhancements into releases based on SEBI's business and technical priorities. Supplier may include in each release emergency maintenance fixes, and/or critical bug fixes available but not yet implemented. In the case of a release containing maintenance patches and enhancements only the portion of the release that would otherwise have constituted an Enhancement will be treated as an Enhancement, unless otherwise approved by SEBI.

Replacement equipments shall be covered under warranty for a three-month period, or the time remaining in the Warranty Period for the item replaced, whichever is greater. The Warranty Period for replacement Software shall be identical to the initial warranty period for the defective Software unless otherwise specified in the contract. During the Warranty Period, the Supplier will provide at no additional cost to SEBI all Product and documentation updates and new software version releases within 15 days of their availability.

3.3 Compliance to Specifications

All the hardware specifications mentioned in the RFP are the required minimum, higher or better specifications would be acceptable. Components furnished shall be complete in every respect with all mountings, fittings, fixtures and standard accessories normally provided with such component's and/or needed for erection, completion and safe operation of the component's as required by applicable codes though they may not have been specifically detailed in the technical specification, unless included in the list of exclusions. All similar standard components/parts of similar standard components provided shall be inter-changeable with one another. The methodology of installation work to be adopted has to ensure minimum damage to the existing structure of the building. Any damage to the existing flooring/ walls/paint etc. shall be made good by the selected bidder. The selected bidder shall be responsible for providing all materials, components, and services, specified or otherwise, which are required to fulfill the intent of ensuring operability, maintainability, and reliability of the complete component covered under this specification within his quoted price. This work shall be in compliance with all applicable standards, statutory regulations and safety requirements in force of the date of award of this contract. The selected bidder shall also be responsible for deputing qualified personnel for installation, testing, commissioning and other services under his scope of work as per this specification. All required tools for completing the scope of work as per the specification is also the responsibility of the selected bidder. The selected bidder shall perform the services and carry out its obligations with all due diligence, efficiency and economy in accordance with generally accepted professional techniques and practices and shall observe sound management practices and employ appropriate advance technology and safe methods. The selected bidder shall always act in respect of any matter relating to this contract or the services as faithful advisers to SEBI. The selected bidder shall furnish complete, well-fabricated and reliably operating and secure systems to SEBI. Design and selection of component and software shall be consistent with the requirements of long term trouble free operation with highest degree of reliability and maintainability. All components shall be constructed to operate safely without due heating, vibration; and all software shall be proven, tested and reliable.

3.4 Maintenance

The bidder shall undertake to maintain the Total Solution for a minimum period of three years from the date of the expiry of the warranty period, However, SEBI

reserves right to enter into AMC for one or more years after Warranty at the finalized price and terms. If the Bidder fails to offer AMC for Three years, then the Bid is liable for rejection.

The bidder should quote separately for annual comprehensive maintenance of hardware and software at site for THREE years from the date of expiry of the warranty period (post-warranty). This rate should be quoted as:

- 4th year comprehensive AMC charges in Indian rupees.
- 5th year comprehensive AMC charges in Indian rupees.
- 6th year comprehensive AMC charges in Indian rupees.

The scope of work for the maintenance period shall include:

The correction of any defects that may arise from the design or workmanship or from any act or omission of the Supplier that may develop under normal use of the supplied Systems. Normal operating environmental conditions shall be specified in the Contract. On receiving the notification from SEBI, the Supplier should carry out the repair / replace the defective systems within a reasonable period of time. This reasonable period of time will be decided by SEBI at the time of entering into a Contract with the successful bidder. This will be done at no extra cost to SEBI. Failure to remedy the defects within the period specified in the Contract, may involve remedial action by SEBI at the Suppliers' risk and expense and without prejudice to any rights that SEBI may have against the Supplier under the Contract.

Corrective maintenance

Preventive maintenance

The offer must give commitment to provide maintenance at the price quoted for THREE years (mention rates separately for each of the three years) from the date of expiry of three-year warranty.

The AMC payment shall be released quarterly in arrears. SEBI reserves right to enter into AMC for part or full project/items.

As part of the maintenance contract, the Supplier will provide software updates, releases, upgrades, version upgrades, versions, bug fixes, patches etc. of all the Application/system Software and Custom Software included in the Products/Bill of Materials of upgrade and also carry out its implementation.

SEBI may decide to outsource the maintenance of the systems to a third-party or SEBI may decide to perform the maintenance in-house. In such case, the Supplier will undertake to provide to the persons / agencies, authorized by SEBI for the purpose, requisite maintenance training, technical know-how kits, and expert assistance on terms mutually agreed upon between SEBI and the Supplier.

The Supplier acknowledges that the IMSS performs a very important oversight function and that continued availability of all of the functionality of the IMSS plays an integral role in the effective discharge by SEBI of some of its functions. Hence Supplier agrees that the services provided by the Supplier in relation to the technical support and maintenance would be subject to a service level agreement and appropriate service level commitments. The Supplier agrees that in the event that the Supplier defaults in meeting such agreed service level commitments, in addition to the other remedies that SEBI has, SEBI shall also be entitled to Service level credits as may be agreed to between the Parties.

SECTION 4

4.1 Bidders Response Sheet

The technical evaluation of the bids will be done on the basis of following broad criteria:

- Bidder capability including proven relevant experience – 25 %
- Core systems – Production servers – POC - 25 %
- Understanding of SEBI's requirement and proposed Solution Architecture (Hardware,Software,Network and Security etc) – 50 %

A. INTRODUCTION

1 Purpose

Objectives
Scope

2 Management Summary

Overview of Bidder
Overview of Proposed Total Solution
Overview of Proposed Time-table and Project Management provisions
Overview of Proposed Maintenance and Support Arrangements

3 Bidder

The registered name of the Bidding company and business address for correspondence
Location
Street
Locality
City
Pin Code
Country
Telephone
Facsimile
Email
Other

4 Contact Name of the Bidder

5 Contact's Position with Bidder

Contact addresses if different from above

Location

Street
Locality
City
Pin Code
Country
Telephone
Facsimile
Email
Other
Business Structure
Bid Company's Registered Address

6 Details of company registration

Names of Directors
Chairman
President/Managing
Director
Directors

Include a structure chart reflecting the organisation

Chart

B. BIDDER CAPABILITY INCLUDING PROVEN RELEVANT EXPERIENCE

1. Financial standing of the Bidder

Following Information from the audited balance sheet of the bidder:

	2006-07	2007-08	2008-09	2009-10
Sales and Other Income				
EBIDT				
Depreciation				
Interest				
Tax				
PAT				
Capital Employed				
Equity				
Net worth				
Total outstanding debt				

2. Defined relationship between OEM Business partners

SEBI appreciates the fact that, as the lead bidder needs to source the items from different OEM partners, they may come together as a consortium to bid for this RFP. However, it is important for SEBI to understand how various project activities have been allocated to different partners and who will be responsible for coordination and project management.

Bidders must define such relationship giving description of allocation of the important project activities to individual partners.

Bidders should also describe the nature of past association amongst partners giving details of any assignments they have worked together for, and the nature of activities partners have carried out in such assignments.

3. Bidder's Relevant Past Projects

Details of at least two similar implementations/upgrades in the recent past (including contact details) which will demonstrate the Bidder's ability to carry out the functions which they are projected to supply in this project in a timely and professional manner.

- a. Project Name with brief description:
- b. Project Location:
- c. Client Name:
- d. Client address:
- e. Client contact/reference person(s):
 - Name
 - Address – if different from above
 - Telephone
 - Facsimile
 - Mobile Phone
 - Email address
- f. Project start date (month/year):
- g. Project elapsed time – months:
- h. Man-months effort, if applicable
- i. Size of the project (Rs. In Cr)
- j. Size of existing customers in terms of trading volumes
- k. Name of senior project staff:
 - Project Director
 - Project Manager

C. SOLUTION ARCHITECTURE AND IMPLEMENTATION METHODOLOGY

1. Designated Staff for the project

A Details of project persons

- Name
- Position
- Project Designation

B Skill levels of staff to be deployed on the project/upgrade

2. Requirements Understood by the bidders

3. Description of Solution Architecture and Design

Bidders are required to give a detailed description of their proposed Solution Architecture for the IMSS infrastructure upgrade. This description must contain the list of different system structure like security modules, network architecture, operational VLANs etc, and how these interface with each other. It is desirable to show an schematic diagram for this purpose. Description of the Solution Architecture should clearly highlight any functionality / performance / usage constraints, if any, imposed by the offered layers of each of the proposed system software layers offered in the solution.

4. Implementation Plan and methodology

A Vendor Support

B Implementation Schedule (Time Frame in Months)

- a Estimated Time to install and configure system in man months
- b Performance Monitoring
- c Conducting User Acceptance Tests

C Upload/Implementation of existing configuration and policies

D User Procedures

E Training

F Documentation Support

5. Project Execution

a. Effort Estimation

Sr. No.	Activities	Person Months	Remarks
1	Hardware Installation (Main + DR + Data sources)		
2	Networking Installation(Main + DR + Data sources)		
3	Products – Software Components		
4	Customisation of software		
5	Integration & Interfaces		

6	Ancillary Services (Cabling Documentation & Training etc.)		
7	Others		
	Total		

b. Performance & Estimated Response Time

Sr. No.	Activities	Response Time (mins.)	Remarks
1	Data Processing (Collection, Transformation & Uploading)		
2	Others		

- 6. Service Level Commitments
- 7. Compliance to terms and conditions
- 8. Integration and interfacing to retained components

D. Proof of Concept

E. Bidder Response Sheet Technical Solution

The bidder shall provide the technical specifications of the solution in the following format. These specifications will form the part of evaluation process and should be used for generation of a complete Bill of Material.

The bidder shall provide the technical specifications of the solution in the following format. These specifications will form the part of evaluation process and should be used for generation of a complete Bill of Material.

Network / Schematic Diagram

Bidder shall submit the complete solution architecture in a form of a Network/Schematic Diagram depicting various systems components. An indicative list of features and systems components is as follows.

Features:

- Single Sign ON
- Flow of Information & connectivity to external entities
- Network Security

System Components:

- Servers
- Storage
- Network Equipments
- Any other components to meet the solution requirement

- Softwares/Utilities
- Backup devices

Specifications of Hardware Components at all locations (Data Centre Mumbai, DR site Chennai and Data sources (NSE, BSE, NSDL, CDSL, MCX etc.)

Functionality (\$): Bidder must indicate the exact functionality of each server proposed as part of the solution

Est. TPC Ratings (%): Bidder to provide an estimate of transaction processing envisaged for each proposed serves where applicable

Specifications (#): Bidder must ensure that the server specification is as per the indicative list mentioned herewith. Bidder may expend the list where applicable.

a. Servers

Sr. No.	Functionality (\$)	Est. TPC Ratings (%)	Specifications (#)	Nos.	Remarks
1			Model No: No. of CPUs Memory (RAM) No of Disk Drives O.S IO Bandwidth TPCC/ TPC-H Ratings HA Cluster(Y/N) Hardware Redundancy Upgrade Path CPU Memory (RAM) Range Disk Drive Range Others		

b. Storage Solution

Sr. No.	Specifications (#)	Nos.	Remarks
1	Model Usable Disk Space Fibre channel – Disk Type No. of Disks Raid Type Storage management Software Expandability Total Storage Capacity Disk Type.		

c. Data Backup at DR site Chennai

Sr. No.	Specifications (#)	Nos.	Remarks
1	Number of Drives Autoloader (Y/N) Number of cartridges Media capacity Data Transfer rate Failover options Remote Data management Expandability		

d. Any Other Hardware/software to meet the solution

Sr. No.	Components	Functionality	Specifications	Nos.	Remarks
1					
2					
...					
N					

e. Network and security equipments at Data Centre Mumbai, Data Sources (NSE, BSE, NSDL, CDSL, MCX) and DR site, Chennai

*Bidder may note that the proposed Network diagram is placed at **Annexure D**. However, if the bidder has a better and more elegant "Network Architecture" he/she is free to propose the same.*

Sr. No.	Components	Specification(#)	Nos.	Remarks
1	Firewall & IDS/IPS			
2	Routers	WAN ports LAN Ports ISDN Ports Memory (RAM/Flash) Scalability		
3	Switches	Model Layer – 3, Layer 2 No. of Ports		
6	Security Solution	IDS, IPS, HIDS, Servers, USB Tokens, etc.		
7	Any Other			

f. Software/Applications/Utilities

Sr. No.	Components	Specification(#) Name & version, Key Features & Supporting white papers	No of Licence	Remarks
1	Operating system with all utilities, tools & required compilers			
2	Databases			
3	Softwares/utilities			
4	Any Other Software to meet the Desired Solution			

g. Ancillary Services:

Sr. No.	Services	Specifications	Remarks
1	Structured Cabling (Data Centre, DR Site, Data sources) if any		
2			

h. Project Management

Sr. No.	Services	Specifications	Remarks
1			
2			
3			

SECTION 5

COMMERCIAL TERMS AND CONDITIONS

Introduction

This section lays down the general and commercial terms and conditions and describes the bidding process including content and form of responses.

5.1 General Terms and Conditions

The bidders are advised to study all technical and commercial aspects, instructions, annexure, terms and specifications in the proposal carefully. Failure to furnish all information required in the Tender Document or submission of a bid not substantially responsive to the Tender document in every respect will be at the bidders risk and may result in the rejection of the bid.

The proposed solution should be cost effective and should provide high availability, both hardware and software, as applicable to the commercial environment.

The specifications mentioned in Annexure B are the minimum requirement of the purchaser and the bidders are free to offer goods with higher configuration.

The components of the proposed solution should be of Original Equipment Manufacturers (OEM) Equipment /Products only. All items to be supplied should conform to industry, compatible with OPEN standards and should be of latest model and original make.

The quotations shall be submitted strictly in conformity with the specifications given in this tender document and as per mandatory response format.

The tenders not submitted in the prescribed format or incomplete in any manner are likely to be rejected

Tender document is not transferable.

Quotations submitted after due date or incomplete in any respect are liable to be rejected.

Technical bid would be opened first. SEBI reserves the right not to process the Commercial Bids in case the Technical Bid is found to be unsuitable / not fulfilling the requirements as specified in the tender document.

The equipment/products quoted should not be from the discontinued production line. In case of discontinuation of the production line after the issue of purchase order, the bidder shall supply the next higher configuration on the same terms.

In case of any reduction in the price due to Government levies/duties/OEM prices, bidder should offer the price reduction to SEBI on all the Components of the proposed solution scheduled to be delivered after one week of the effective date of such announcement. For this purpose, Bidder should voluntarily intimate such price reduction to SEBI, produce the document of OEM's listed price and the discounted price offered to SEBI.

All the standards related to the solution proposed are to be Compliant as per the best industry standard.

The bidder will, by responding to SEBI for RFP, be deemed to have accepted the terms and conditions of the RFP.

5.2 Rights of SEBI

This RFP entails an invitation by SEBI for bidder response for the upgrade of IMSS IT infrastructure. It does not imply an offer by SEBI. Thereby, there will be no contractual obligation until a formal contract is executed by the authorized signatories of parties, SEBI and the selected bidder.

With regard to the RFP, SEBI has the following rights:

- Accept or reject any of the proposals.
- Alter the RFP.
- Ask for re-submission.
- Request clarification from bidders.
- Terminate the RFP process, partially or entirely.
- Modify the specifications during the process and even after bidder selection.
- to obtain revised price Bids from the Bidders with regard to changes in RFP clauses
- to negotiate with any or all Bidders
- to accept any Bid in whole or in part
- to split orders in favour of more than one Bidder
- to release order, part order or more than one order
- to finalize the bill of material and repeat orders.
- to evaluate the Bids based on reasonability and workable offer, especially with regard to Annual Maintenance solution under this RFP.

SEBI reserves the right to issue the amendments to the RFP at anytime, prior to the deadline for the submission of Bids. From the date of issue, amendments to RFP shall be deemed to form an integral part of the RFP Document.

The Bidders shall arrange to give a presentation/demonstration on their solution after submitting their Bid, if required by SEBI. SEBI shall communicate the venue, duration, date and time of presentation/demonstration to the Bidders at a later stage. All costs and expenses incurred by Respondents in any way associated with the development, preparation, and submission of responses, including but not limited to; the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by SEBI, will be borne entirely and exclusively by the Respondent

SEBI may, in its absolute discretion, engage in discussion or negotiation with any Respondent (or simultaneously with more than one Respondent) after the RFP closes to improve or clarify any response.

SEBI may, in its absolute discretion, seek additional information or material from any Respondents after the RFP closes and all such information and material provided must be taken to form part of that Respondent's response.

The Bids received and accepted will be evaluated by SEBI to ascertain the best and lowest Bid in the interest of SEBI based on evaluation process described in this RFP. However, SEBI does not bind itself to accept the lowest or any Bid and reserves the right to reject any or all Bids at any point of time prior to the order without assigning any reasons whatsoever. SEBI reserves the right to re-tender. SEBI shall not incur any liability to the affected Bidder(s) on account of such rejection. SEBI shall not be obliged to inform the affected Bidder(s) of the grounds for SEBI's rejection. It is to be understood clearly by the Bidders that the selection process requires them to have adequate expertise in the proposed technology. SEBI while evaluating the proposed solution will also consider the competence and capability of the Bidders in design, implementation and support services.

Site visits may be sought at the discretion of SEBI. Bidders shall provide, in addition to customer sites, an invitation to SEBI to visit Bidder's own development site for conducting POC. SEBI will bear all traveling, lodging, boarding costs of its officials in relation to such visits.

5.3 Clarification on RFP

The Bidder shall carefully examine and understand the specifications /conditions of RFP and seek written clarifications, if required, to ensure that they have understood all specifications/conditions of RFP. Written requests for clarification may be submitted to SEBI to the address given in section 5.9 below or **at imss@sebi.gov.in** within 15 days from the date of issue of this RFP along with the bidder credentials/profile as given in eligibility criteria. Bidders are requested to see the inputs provided in section 4 (Bidder's Response Sheet) for providing the aforesaid bidder credentials/profile.

Thereafter, within 10 days, SEBI shall convene a Bidders meeting in which the bidders need to demonstrate through presentations and technical discussions their capability and technical competence to deliver the requirements. The same needs to be submitted as a response to RFP including the key resources deployed during the installation and maintenance. During meeting SEBI and its technical committee will clarify all queries raised by the Bidders. Only the eligible bidders shall be present during the said time. No individual consultation shall be entertained. The Bidder shall collect clarified points in writing from SEBI within two days from the date of the meeting. No more clarification other than that asked during or before the above meeting shall be entertained. No oral consultation other than during the meeting shall be entertained. SEBI reserves the right to communicate to all the bidders the response of the question raised by any particular bidder.

The Bidder's Bid should not carry any sections like clarifications, 'as orally told', 'to be discussed', interpretations and assumptions. With the submission of the Bid, the Bidder acknowledges that he/she has carefully studied and understood the RFP in complete.

5.4 Prices

The price quoted should be inclusive of all Central/State Government levies, taxes, sales tax, excise duty, custom duty, VAT and insurance charges with three years warranty, excluding Octroi, which, if any, shall be paid as per the actual on production of relevant documents (Billed to SEBI only), in original.

The prices quoted by the bidders shall be in Indian Rupees, only

The Bids shall be valid for a period of ONE YEAR from the closing date for submission of the Bid.

5.5 Payment Terms

Unless otherwise stated the general terms of payment are:

- a) 50 % of the Component value on Delivery
- b) 40 % of the Component value on Installation & Acceptance
- c) 10% of the Component value against performance bank guarantee.

Billing for Hardware, Network and System Software Implementation:

The Invoices/ bills will be raised as per the following Milestones. Milestone Percentages are with reference to the Total Amount quoted under **Bill of Materials**.

Milestone	Description	Milestone percentage
1	Delivery of Hardware/ system software components/ Network Components	50%
2	Installation and acceptance of Hardware/ system software components/ Network Components	25%

3	Payable on final acceptance Hardware/ system software components/ Network Components against performance bank guarantee	25%
---	---	------------

Billing for Ancillary services and project management

The Invoices will be raised as per the following Milestones. Milestone Percentages are with reference to the Total Amount quoted under **Bill of Materials**.

Milestone	Description	Milestone percentage
1	Final Acceptance of Upgrade	90%
2	Payable on final acceptance against performance bank guarantee	10%

All the payments as above shall be paid to the vendor by SEBI, after deducting the amounts towards Tax Deducted at Source (TDS) wherever applicable as may be specified by Government in this behalf, at such rates prevalent at the time of making respective payments.

5.6 Performance Bank Guarantee

The Bidder shall at his own expense furnish within 30 working days from the date of signing of agreement an unconditional and irrevocable Performance Bank Guarantee (PBG) for 10% of the Agreement/ contract value, in favor of SEBI, from a scheduled Bank towards the due and punctual performance and fulfillment of the Agreement/ contract in accordance with the specifications and conditions of the RFP and agreed upon on final Bid evaluation. The format is given in **Annexure E**.

The performance bank guarantee will be valid till the end of the warranty period under the agreement/ contract. Subject to the terms and conditions in the performance bank guarantee, at the end of the warranty period, the PBG will lapse automatically. The guarantee shall contain a claim period of three months from the last date of validity. PBG may be discharged by SEBI upon being satisfied that there has been due performance of the obligations by the Bidder.

The Bidder shall be responsible for extending the validity date and claim period of all the bank guarantees as and when it is due on account of incompleteness of work under guarantees. SEBI shall invoke the guarantee before expiry of validity if work is not completed and the guarantee is not extended, accordingly.

5.6 Delays in the Vendor's Performance

The Vendor must strictly adhere to the implementation schedule, as specified in the agreement/ contract in the performance of the obligations and any delay in this regard will enable SEBI to resort to any or both of the following:

- a) Claiming Liquidated Damages

b) Termination of the agreement/contract fully or partly and claim liquidated damages.

Liquidated Damages

Time is the essence of the Agreement/ contract. The Vendor will be liable to pay SEBI liquidated damages (LD) @ one percent (1%) per week but limited to the maximum of 10% on unexecuted value of agreement/ contract inclusive of all taxes, duties, levies etc. due to any delay in performance or non-performance of any or all the obligations under the agreement/ contract. This condition will not be applicable for reasons attributable to SEBI as well as Force Majeure, though the onus of proving the same lies with the Vendor.

SEBI will have the rights to recover the liquidated damages, if any, from any amount payable to the Vendor. Also, if the specifications of the RFP are not met by the Vendor during various tests, the Vendor shall rectify or replace the same to comply with the specifications immediately to ensure the committed uptime, failing which SEBI has the sole right either to reject or to accept it finally by recovering the suitable amount as deemed reasonable by SEBI. Non compliance of uptime shall result in extending the Warranty Period on pro-rata basis or recovering the suitable amount as deemed reasonable by SEBI.

5.7 Delivery, Installation and Commissioning

All the goods or products under the Agreement/ contract shall be delivered, installed and accepted at the final destination specified by SEBI in this regard **within 4 (four) calendar months from the date of award of contract to the selected bidder (4-6 weeks delivery, 2 months installation, configuration, acceptance and commissioning)**. All the costs till the time the goods or products are delivered shall be borne by the Bidder. All the documents like Invoice, Packing list, Guarantee Certificates, Bidders' inspection reports, Insurance certificate, certificate of origin, etc. will need to be produced by the Bidder to SEBI. The Bidder is also responsible for the goods/products until their acceptance by SEBI.

The Bidder shall be responsible for installation and commissioning of the Systems including cabling and other related activities such as unpacking, uncrating, inspection etc. for which SEBI shall provide the required space. While unpacking and installation the Bidder shall check physical availability of items as per the packing list. Delivery of goods or products shall be deemed to have been made when the contents of the cases, boxes or packages are witnessed together by SEBI and the Bidder or their representatives, to be identical to those listed in the packing list included therein. Delivery is considered complete once the items are installed. However, this proof of delivery to the final destination shall in no way absolve/release the Bidder from the performance of his warranty obligations under the agreement/ contract.

5.8 Insurance

The Bidder shall fully insure each and every goods or products supplied under the total solution against all risks including terrorism, riots and civil commotion, up to the point of acceptance or up to 30 days from actual delivery (i.e. installation), whichever is earlier, with an insurance company/corporation.

The goods supplied under the Agreement/ contract shall be fully insured in Indian Rupees naming SEBI as the beneficiary. In case of any loss or damage occurs, the Bidder should be responsible for initiating and pursuing claims and settlement and simultaneously also make arrangements for repair and/or replacement of any damaged item/s.

5.9 Submission of Bids

The Bidders should submit their responses in two parts,

1. The Technical Bid
2. The Commercial Bid.

Both the Bids shall be sealed and submitted separately. Formats of the technical and commercial tender forms are placed at **Annexure F and G** respectively.

All Bids and supporting documentation shall be submitted in English. All costs and charges indicated in the Commercial Bids should only be in Indian Rupees.

Bidders should provide their Technical and Commercial responses in one original and six copies and shall be labeled as "Original" or "Copy" as appropriate. Each of these shall then be sealed in a separate envelope labeled "Original Tender" or "Copy Tender" as appropriate. All the sealed envelopes containing Technical responses shall then be sealed in one envelope marked "Technical Bid for IMSS IT infrastructure upgrade against RFP no SEBI/IMSS/2011/01 dated 02/08/2011" in the top left hand corner. Similarly all the sealed envelopes containing Commercial responses shall be sealed in another envelope marked "Commercial Bid for IMSS against RFP no. SEBI/IMSS2011/01 dated 02/08/2011 NOT to be opened before Technical Bid opening and evaluation" in the top left hand corner.

The Bids which are not sealed as indicated above are liable to be rejected. SEBI will not be liable for Postal or any other delay, non-receipt/non-delivery of documents, loss of documents in transit, etc., if any, in the Bidder receiving the RFP and/or in submitting the Bid.

Bidders are requested to submit a "softcopy" version of their Technical and Commercial responses on a CD in Microsoft Office 97 format. Softcopies are to be sealed within the respective Technical and Commercial Bid envelopes.

All pages of the Bid including Brochures are to be numbered as *Page --- (current page) of --- (total pages)*. The numbering shall be done for the whole Bid and not section-wise.

The envelope shall be dated with the current date in the top right hand corner and addressed as below:

Mr. S Ramann
Officer on Special Duty
Securities and Exchange Board of India
Fifth Floor, SEBI Bhavan“A” Wing,
Bandra Kurla ComplexBandra (East) - 400 051
India.

- Please note that in the event of any discrepancies between the 'Original' and the 'Copy' of the Technical Bid or the Commercial Bid, the Original shall govern.
- Bids sealed as above should be delivered to the address mentioned above on or before 3:00 p.m. on September 09, 2011 Bids may be sent by registered post or hand delivered. Bids received after 3:00 p.m. on September 09, 2011 will not be accepted by SEBI, under any circumstances. The Technical Bids will be opened on the same day. This will be done in the presence of all the Bidders.
- The Technical Bid shall be accompanied by Earnest Money Deposit (EMD) of Rs.10,00,000 (Rs.TEN LAKHS Only) by way of Demand Draft of a Scheduled Bank in favour of "Securities and Exchange Board of India" payable at Mumbai. No interest shall be allowed on the Earnest Money. Bids without Earnest Money Deposit are liable for rejection.
- The EMD should not be placed in the Commercial Bid envelopes. Submission of EMD in the Commercial Bid envelope shall render the Bid being rejected on the grounds of non-submission of EMD.
- The EMD shall be returned to the selected Bidder on his/her submission of Performance Bank Guarantee, as indicated in **Annexure E**. For other Bidders, the EMD shall be returned not later than awarding of contract to the selected Bidder.
- All Bidders, or their authorized representatives, shall be present at the time of the opening of the Technical Bid. Only two persons per Bidder will be allowed to be present at the time of the opening the Technical Bids.
- The cost of preparing the response to this RFP will be the responsibility of the Bidder and SEBI will not be liable for any costs incurred by the Bidder.
- Incomplete Bid(s), conditional Bid(s), Bid(s) not conforming to the terms and conditions, Bid without EMD are liable for rejection by SEBI.
- If the submission does not include all the information required or is incomplete, the proposal is liable to be rejected.
- All submissions, including any accompanying documents, will become the property of SEBI. Recipients shall be deemed to license, and grant all rights to SEBI to reproduce the whole or any portion of their submission for the purpose of evaluation, to disclose the contents of the submission to other Recipients and to disclose and/or use the contents of the submission as the basis for any resulting RFP process, notwithstanding any copyright or other intellectual property right that may subsist in the submission or accompanying documents.

SECTION 6

Annexures

Annexure A

Benchmarking for performance

Benchmarking objective: to run the alert program of IMSS and measure the performance/response time

Data range for conducting benchmarking : 15 days

Data range for conducting Alerting : 1 day

Total data range for each run :16 days

Activities:

Day	Tasks
Day 1	Setting up the benchmarking environment <ul style="list-style-type: none">• Server installation(OS installation, data partitioning etc)• Installation of SMARTS application software.• Loading of data for required for benchmarking and alerting.• Testing of environment
Day 2	<ul style="list-style-type: none">• Conducting Benchmark runs (two times)
Day 3	<ul style="list-style-type: none">• Additional runs• Preparation of reports
Day 4	<ul style="list-style-type: none">• Day reserved for handling contingency

Annexure B

Proposed Technical specifications

S/N	Item	Proposed Configuration/specifications	Existing configuration/specification
1	Support Servers	<p>Server specification should have minimum configuration given below and are not limited to: Processor: latest generation, quad-core or higher (2.4 GHz, 1333 FSB), 12 MB L3 Cache per socket, 1076/1600 MHz FSB , 8 GB DDR-III 1066 MHz, ECC memory, upgradable to 48 GB RAM, 2*600GB SAS, H/S, HDD's 10k rpm, 6 GBPS. Or Higher HDD,DVD R/w, internal drive RAID controller(RAID 0/1/1+0/5/5+0), Windows Server 2008 and Latest LINUX version Certified Preferably Blade server at SEBI datacenter and DR site. Vendor may propose appropriate servers at data sources</p>	HCL Infiniti Global Line 2765 XD Server Intel Xeon 2. 4 GHz. / 512 KB Cache/ 400 FSB, 2x 18 GB Ultra 3 Hot Swap HDD ,Dual Channel RAID Controller,OS:Window 2003 server/Linux
2	Network and security components	All Network Components to Support Giga Bit Computing	
2A	Routers	<p>Features of router should included but not limited to: Physical attributes o The modules, power supply should have support for hot swappable functionality. o Modular Chassis o Router performance should be minimum of 400 Kpps o Power supply for 230 V AC 50 Hz with Redundant power supply Architecture o The architecture should be based on high performance, multicore Processor o The Router should be a single box configuration and should be modular, so that there is flexibility to use the appropriate choice of interfaces as and when required. o It should support high powered service modules, Gigabit Ethernet switching. o It should support energy monitoring and</p>	Cisco 2651/2691/3725 routers

		<p>control capabilities while enhancing overall system performance.</p> <ul style="list-style-type: none"> o It should support embedded hardware encryption acceleration. o Should support high speed WAN deployment requirement up to 25Mbps with services enabled o It should support a fabric which will allow high-bandwidth module-to-module communication without compromising routing performance. o Should provide out of band management access via Aux or console o Should support direct console access via USB interface o Should be NEBS compliant <p>Interface / Slots</p> <ul style="list-style-type: none"> o Should support upto 2 onboard 10/100/1000 Ethernet routed port o Interfaces like E3, Ch-E1, and E1 G703 Interfaces as per ITU-T Standard. o At least two spare ports(on board port) for 8 Mbps leased lines and ISDN line termination o Console port 1 numbers <p>Security</p> <ul style="list-style-type: none"> o GRE and IP Sec 3DES/AES VPN for configuration of VPN tunnels. o Support for IPSEC Site-to-Site and Remote Access VPNs. Should provide a hardware assisted IPsec 3DES encryption performance up to 400 Mpps. o NAT, PAT o Access control - Multilevel o Support ACL's to provide supervision and control. o Multiple Privilege Levels for managing & monitoring o Support for Remote Authentication User Service (RADIUS) and AAA o Controlled SNMP Access using ACL on router to ensure SNMP access only to identified NMS/EMS o PPP CHAP support. PAP (optional) o DoS prevention through TCP Intercept & DDoS protection <p>Protocol support</p> <ul style="list-style-type: none"> o IPv4, IPv6, Static routes, Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), BGP Router Reflector, 	
--	--	---	--

		<p>Multicast Internet Group Management Protocol (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Generic Routing Encapsulation (GRE),IPSec, IPv4-to-IPv6 Multicast, MPLS, Encapsulation Support802.1q VLAN, Point-to-Point Protocol (PPP),Multilink Point-to-Point Protocol (MLPPP),ATM, Frame Relay, Multilink Frame Relay (MLFR) (FR.15 and FR.16),High-Level Data Link Control (HDLC),Serial (RS-232, RS-449, X.21, V.35, and EIA-530),Point-to-Point Protocol over Ethernet (PPPoE)</p> <p>Network Management</p> <ul style="list-style-type: none"> o IP SLA or equivalent, SNMP support o It should support device and system management feature that helps to customize behavior based on network events as they happen & execute scripts if required o Should support online diagnostics on hardware components o RMON, Syslog and Netflow or equivalent 	
2B	Switches	<p>Core switch: Layer – 3 and support switches(Layer 2)</p> <p>Features should included but not limited to:</p> <ul style="list-style-type: none"> o Redundant Supervisor / Switching / Routing engine. All the Relevant hardware should be loaded to achieve the required Switching & routing performance. o Internal Redundant Power Supply o Power supply 230 Volt 50Hz input o Modular Chassis <p>Support for 10/100/1000 Mbps and upgradable</p> <p>Manageability & Up gradation</p> <p>Console port for administration & managemento Support SNMP v1, v2o Support management using CLI, GUI using Web interfaceo Support FTP/TFTP for upgrading the operating Systemo Prioritization of the network Traffic Fiber Uplinks.</p> <p>Features</p> <ul style="list-style-type: none"> o The Switch should have a 2TBps of switching capacity scalable up to 4TBps o The Switch should have Switch fabric 	Cisco 3750/2950 switches

		<p>redundancy</p> <ul style="list-style-type: none"> o One line card with 24 port SFP Fibre Gigabit Ethernet populated with 15 1000BASE-T SFP module and 5 1000BASE-SX SFP transceiver module for MMF. <p>switch should be NEBS Compliant</p> <ul style="list-style-type: none"> o Should support up to 240 1 GE ports o Should support up to 82 10GE ports o Should support up to 20 40GE ports o Should support at least 720Mpps of IPv4 Routing in Hardware o Should support at least 390Mpps of IPv6 Routing in Hardware. o Should Support 128,000 MAC addresses o Should support at least 4096 Vlans in hardware. <p>the platform should support up to 8192 VRF's</p> <ul style="list-style-type: none"> o Platform should support virtualization at Layer 2 without affecting the Forwarding Performance o Platform should support virtualization at Layer 3 without affecting the Forwarding Performance. o The platform must support switch virtualization without affecting forwarding performance. o The platform must support quality of service (QoS) mechanisms o The Platform must support Virtualization of Layer 4 - Layer 7 services <p>IP Routing Protocols</p> <ul style="list-style-type: none"> o Static Routingo OSPF v2 and OSPF v3o RIP v1, RIP v2, RIPngo HSRP /VRRP o IPv6 support with no additional cost <p>Security</p> <ul style="list-style-type: none"> o Standard and extended ACL's on all ports o AAA and RADIUS authenticationo Secure Shell (SSH) Protocol <p>L2 Features</p> <ul style="list-style-type: none"> o IEEE 802.1Q VLAN encapsulationo 802.1s,o 802.1w,GMP snooping <p>Performance</p> <p>High back plane speed of 600 Gbps switching fabric</p> <p>Switch should be loaded with required</p>	
--	--	--	--

		hardware to provide forwarding rate of 300 Mpps (non-blocking) Other features should support hardware based Firewall and Intrusion detection services as and when required o Should support hardware based SSL by offloading from server. o Should support hardware based server Load Balancer	
--	--	---	--

2C	Firewalls	<p>Firewall (Primary & Failover)-latest series Features should be included but not limited to: As per the specifications of CERT-IN- Failover / Hot Standby Packet Filters and Stateful, Multi-Layer Firewalls Application and Circuit Level Gateways Adherence to defined Security Policy Protection from Denial of Service (DoS) attacks Ease of Administration Remote Administration.</p> <p>External Firewall Physical attributes o Should be mountable on 19" Rack, Modular Chassis o The firewall should have Dual Hot Swappable power supplies o 4 x GE, upgradable to 8 x GE, the platform should have expansion slots to accommodate Fiber Interface (Fiber SX and LX Interfaces) or Copper interfaces o Firewall appliance should have Console port and USB Ports</p> <p>Performance o Encrypted throughput: minimum 5 Gbps o Concurrent connections: up to 1,000,000 o Simultaneous VPN tunnels o Firewall & Integrated IPSEC VPN Applications should be ICSA Labs certified for ICSA 4.0, FIPS 140-2 certified o The Firewall VPN AES throughput should be more than 2 Gbps o The Firewall must support more than 32,000 new sessions per second processing.</p> <p>Routing Protocol o Static Routes o RIPv1, RIPv2 o OSPF Protocol o TCP/IP, PPTP, RTP, L2TP, IPsec, GRE, DES/3DES/AES o PPPoE, EAP-TLS, RTP, FTP, HTTP, HTTPS o SNMP, SMTP, DHCP, DNS o Support for IPv6 with no additional cost</p> <p>Other support o 802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, support VLAN,</p>	<p>External firewall: Alteon Switched Firewall 5409 Components: Switched Firewall Accelerator 5400, Switched Firewall Director 5009</p> <p>Internal firewall: Cisco PIX 515 E</p>
----	-----------	--	--

		<p>Layer 2 Firewall, Radius/ TACACS</p> <ul style="list-style-type: none"> o It should enable blocking of Peer-Peer applications, like Kazaa, Gnutella, Bit Torrent, IRC (over HTTP) <p>QoS</p> <ul style="list-style-type: none"> o QoS Support [Guaranteed bandwidth, Maximum bandwidth, Priority bandwidth utilization, QOS weighted priorities, QOS guarantees, QOS limits and QOS VPN. <p>Management and reporting specifications</p> <ul style="list-style-type: none"> o Console, Telnet, SSHv2, Browser based configuration o Firewall Real-Time Monitoring, Management & Log Collection (with storage) should be a SINGLE Appliance / Server o Logging and Report Generation. o Proposed Solution should be distributed on multiple tiers, with separate components Firewall Modules, Firewall Management & Monitoring Server and GUI Console <p>The communication between all the components of Firewall System (firewall module, logging & policy and WebUI Console) should be encrypted with SSL or PKI.</p> <ul style="list-style-type: none"> o Firewall Management system should also provide the real time health status of all the firewall modules on the dashboard for CPU & memory utilization, state table, total # of concurrent connections and the connections/second counter. o Firewall Real-Time Monitoring, Management & Log Collection (with storage) should be a SINGLE Appliance / Server o The Firewall administration software must provide a means of viewing, filtering and managing the log data. <p>Complete firewall management solution including real-time monitoring, event logs collection, & policy enforcement should be from a single device only (mgt server/appliance).</p> <p>The Firewall logs must contain information about the firewall policy rule that triggered the log.</p> <p>Firewall should have more than 40+ GB HDD</p>	
--	--	---	--

		<p>Internal Firewall Features should be included but not limited to: Physical attributes o Should be mountable on 19" Rack o Modular Chassis o The firewall should have Dual Hot Swappable power supplies Interfaces o The Firewalls should be Hardware based, Reliable, purpose-built security appliance with hardened operating system that eliminates the security risks associated with general-purpose operating systems with 8 Nos of 10/100/1000 Base Tx interfaces expandable to 16 No's of 10/100/1000 and support for 10G (Future) with separate management ports. o The Appliance should be Full-featured, high-performance firewall and should have support for intrusion prevention system (IPS), network antivirus, and IP Security/Secure Sockets Layer (IPSec/SSL) VPN technologies deliver robust application security, user- and application-based access control, worm and virus mitigation, malware protection, and remote user/site connectivity as and when required by SEBI. should be redundant supporting Active/Active or Active/Standby Firewall for High Availability & Scalability o 4 x GE, upgradable to 8 x GE o Console Port 1 number Performance o Encrypted throughput: minimum 5 Gbps o Concurrent connections: up to 1,000,000 o IPSec VPN Peers of 5000 or more o Should include unlimited user support for the VPN Client. Should be available on wide range of platforms, including Microsoft Windows 98, ME, NT, 2000, and XP; Sun Solaris; Intel-based Linux distributions; and Apple Macintosh OS X o VPN Throughput of at least 2 Gbps IPSec remote-access VPN concentrator services for up to hundreds of simultaneous remote software- or hardware-based VPN clients</p>	
--	--	---	--

		<p>Routing Protocols</p> <ul style="list-style-type: none"> o Static Routes o RIPv1, RIPv2 o The Firewall should have support for Integrated specialized inspection engines for protocols like HTTP, FTP, ESMTTP, DNS, SNMP, ICMP, SQL*Net, NFS, H.323 Versions 1-4, SIP, MGCP, RTSP, TAPI and JTAPI over CTIQBE protocol, GTP, LDAP, ILS, RPC and many more <p>Other support</p> <p>802.1Q, NAT, PAT, IP Multicast support, Remote Access VPN, Time based Access control lists, support VLAN, Layer 2 Firewall, Radius/ TACACSQoS</p> <ul style="list-style-type: none"> o Should deliver per-flow, policy-based QoS services, with support for LLQ and Traffic Policing for prioritizing latency-sensitive network traffic and limiting bandwidth usage of administrator-specified applications o Packet Capturing for powerful troubleshooting capabilities by providing robust packet-capturing facilities on each interface. Support for several methods of accessing captured packets, including through the console, secure Web access, or a file exported to a TFTP server. <p>Management and reporting specifications</p> <ul style="list-style-type: none"> o Console, Telnet, SSHv2, Browser based configuration o SNMPv1, SNMPv2 Support for Built-in Management Software for simple, secure remote management of the security appliances through integrated, Web-based GUI. o Should provide a wide range of informative, real-time, and historical reports that give critical insight into usage trends, performance baselines, and security events o Strong authentication of users through the Firewall appliance through a local user database or through integration with enterprise databases, either directly using RADIUS or indirectly with AAA Server real time monitoring of the firewall 	
--	--	---	--

		<p>through the management console or through external syslog servers</p> <ul style="list-style-type: none"> o Support for up to 16 levels of customizable administrative roles, so that businesses can grant administrators and operations personnel the appropriate level of access to each appliance; for example, monitoring-only access, read-only access to the configuration, network configuration only, firewall configuration only, and so on o Ability to generate AAA records for tracking administrative access to appliances, as well as tracking all configuration changes made during an administrative session.. 	
2D	<p>Network Intrusion detection/prevention system(NIDS/NIPS)</p>	<p>Features should be included but not limited to:</p> <p>Action on detection</p> <ul style="list-style-type: none"> o IPS should be available as a plug-n-play appliance. Block attacks in real time, Drop Attack Packets, Packet Logging, Block attacks on SQL injection, LDAP injection, cross site request forgery attacks. (CSRF). o Reset Connections, Action per Attack o Support for detailed intrusion alarms <p>Stateful Operation</p> <ul style="list-style-type: none"> o TCP Reassembly o IP Defragment o Bi-directional Inspection o Forensic Data Collection o Access Lists <p>Signature Detection</p> <ul style="list-style-type: none"> o Vendors Signature Database – minimum 2000 o Should support Automatic signature synchronization from OEM Database server <p>Performance</p> <ul style="list-style-type: none"> o The appliance have inspected throughput of 2.5 Gbps for all kinds of ecommerce and web traffic. o The New Connections per second should be 35,000. o The Concurrent Sessions should be 1,500,000. the appliance should have separate dedicated 10/100/1000 Mbps interface for 	ISS Proventia A1204

		<p>management console. None of the monitoring ports should be used for this purpose.</p> <p>Extensive protocol monitoring: should support monitoring of protocols such as TCP/IP, ICMP, FTP, UDP, SMTP, HTTP, SNMP, DNS, RPC, NetBIOS, Telnet etc</p> <p>Should also have the ability to monitor MPLS and 802.1Q (trunked)</p> <p>Traffic</p> <p>Alerting SNMP, SMTP support</p> <ul style="list-style-type: none"> o Log File, Syslog support Operations o Should support 24/7 Security Update Service o Should support automatic Real Time signature update o Should support Provision to add static own attack signatures <p>Reporting</p> <ul style="list-style-type: none"> o System should provide centralized reporting and management .o System should provide comprehensive security event reporting <p>Management</p> <ul style="list-style-type: none"> o Console, SSH, Telnet, HTTPS / HTTP, SNMP v1, v2 oIPS Management console should support high availability. o Management Console should be able to integrate and correlate with vulnerability assessment solution. o IPS should offer variety of built-in responses including console alerts, database logging, email notifications, SNMP traps, offending packet captures, and packet captures. 	
2E	RSA tokens	50 Tokens of RSA Model SID700 and other related components	SEBI has a RSA 2 Factor Authentication System already in place & integrated with application.

3	Others	<p>IP KVM Switch at DC if required</p> <ul style="list-style-type: none"> o It should have a minimum of 8 ports scalable & upgradeable. o It should support 2 remote users and 1 user at the rack o Remote Access appliance should have the following functionalities o It should take control of servers at BIOS Level o It should facilitate both in-band & out-of band access o It should be able to integrate with power strips, so as to be able to reset power of remote device at port level. o Remote access of both Servers and serial devices such as routers (through same or different appliances). o It should have facility to integrate with secure management device o Gigabit Ethernet ports. virtual Media Support of multiple media including 'ISO image' files o Dual (redundant) Power supply o Dual Ethernet with Failover o PC selection – On screen Display menu hot key o 19 inch Rack mountable design o KVM access over IP o Browser based Management available at both remote and local (Supported Browsers = Internet Explorer for MS-Windows, Firefox for MS-Windows and Linux) o Support for resolution of 1600*1200 or above o Single window access to all equipment. o Equipment access logs and event history and send email alerts based on logs details as triggers o Logging should be centralizable in one Syslog server. o Automatic Mouse Synchronization <p>Network Management Software Generic – Essentially to manage the Network Devices & the Bundled Software with above mentioned devices</p>	8 port KVM switch
---	--------	--	-------------------

4	Storage device	<p>Compatible with Sun StorageTek 6140 array. - Depending upon the solution offered, if HBA card or any other hardware item is required to connect with the existing production servers and storage system, those items also need to be provided.</p> <p>Storage capacity 100TB (600 GB HDD each)</p> <p>Features</p> <p>The storage array should support dual, redundant, hot-pluggable, active-active array controllers for high performance and reliability.</p> <ul style="list-style-type: none"> o Should offer at least 3200 MB/s of backend throughput using either FC or SAS connectivity. <p>Storage subsystem shall be offered with Dual 4Gbps FC ports per controller.</p> <ul style="list-style-type: none"> o Storage array shall support Sustained sequential throughput of 250MB/sec from Disk. o Storage array shall support at-least 200000 IOPS from Cache. o Offered Storage Subsystem shall support Raid 0, 1 , 1+0 , 5 and Raid 6 with Dual Parity Protection. <p>Storage Subsystem shall support minimum of 2048 Logical Units. Storage Array shall also support creation of more than 2TB volume at controller level.</p> <ul style="list-style-type: none"> oMulti-path and load balancing software shall be provided, if vendor does not support MPIO functionality of Operating system. oAtleast 2 Global hot spare drive shall be configured for every 30 drives. 	<p>Sun StorageTek 6140 array. Existing configuration:</p> <ul style="list-style-type: none"> 1 Storage controller. 3 Expansion tray <p>Capacity appx:17TB (53 X 300GB)</p>
5	Backup device	<p>Features should be included but not limited to:</p> <p>Preferably Sun StorageTek SL500 tape library with 3 LTO GEN4 drives & Symantec NetBackup Software version 6.5. The backup system should be scalable for taking backup of data from SEBI's network other than IMSS data.</p>	<p>Sun StorageTek SL500 tape library with 3 LTO GEN4 drives Symantec NetBackup Software version 6.5</p>

6	Production server (SMARTS server)	<p>Features should be compatible to existing configuration /higher version</p> <p>Operating System should be Red Hat Enterprise Linux 5.5 / higher version</p> <ul style="list-style-type: none"> oAMD/Intel High end processor o128 GB RAM, Upgradable upto 256GB o 4 X 300 GB 2.5 10K HDD RAID 1 HDD Server Should Support - Hot-swap SAS/SATA/SSD 	<p>Sun Fire X4140 x64 Server and Sun Fire X4600 M2 x64</p> <p>AMD Opteron Model 2222 (3.0GHz/1MB) dual core processor for Sun Fire X4140 and X4600 M2 x64 servers 8 GB Memory kit DDR2-667 Registered ECC DIMMs (2x 4GB) for Sun Fire X4140 and Red Hat Enterprise Linux 5.1 Advanced Platform, 1-year Standard Subscription for x86, AMD64, 146GB 10K RPM 2.5" SAS hard disk drive</p>
7	SAN Switch	<p>Features should be included but not limited to:</p> <ul style="list-style-type: none"> o 24 port Switch should be configured with required ports activated with redundant power supplies and fans should be configured, scalable to 40 ports o Should deliver 8 Gbit/Sec Non-blocking architecture with 1:1 performance for up to 40 ports in a energy-efficient fashion o SAN switch port count should be considered to support configuration & integration of all FC ports specified in the servers, SAN storage, Tape Library oThe switch shall provide Aggregate bidirectional bandwidth of 680 Gbit/sec: 40 ports× 8 Gbit/sec (data rate) end to end. oSAN switches should support HBA of different OEMs, multiple operating Systems, including, but not limited to HP-UX, IBM AIX, Linux, MS-Window, Sun Solaris etc. The SAN switch should support all leading SAN disk array, VTL and tape libraries including, but not limited to, EMC, Hitachi, HP, IBM, Sun etc o The switch should be configured with required licenses. o Offered SAN switches shall be highly efficient in power consumption o Switch shall support POST and online/offline diagnostics. o The switch should be rack mountable 	NA

Annexure C

Specifications of Existing Hardware components at Data centre, Mumbai, Data sources (NSE, BSE, NSDL, CDSL, MCX) and DR site, Chennai.

SNo./ Item	Make & Version	Qty	Applications Installed	Functionality	Warranty till date
HARDWARE COMPONENTS - DC site, Mumbai					
Firewall server	HCL Infiniti Global Line 2765 XD Server	1	1) ISS Site protector 2) Trend Micro Office scan OS: Windows 2003 server	Core application: ISS site protector used for log collection and monitoring of 2 proventia devices (NIDS).logs are monitored by HCL security operation centre(SOC).	25/02/2012
Firewall server	HCL Infiniti Global Line 2765 XD Server	1	1) Checkpoint Smart console 2) Webtrends Firewall Suite 3) Trend Micro Office scan Client OS:Windows 2003 server	Core application: Checkpoint Smart console provides various utilities of checkpoint application. It contains Smart dashboard application which is used for firewall rules and policies management other application: webtrend firewall suite: produces firewall and web activity reports that detail security violations. Integrated with security application i.e. checkpoint.	25/02/2012
Proxy & URL filtering server	HCL Infiniti Global Line 2765 XD Server	1	1) Squid 2) Interscan Web Security Suite 3) Websense Policy Server 4) Trend Micro Office scan OS: Redhat Linux	Core application: squid: serves all clients for internet connectivity. Core secondary application: websense: acts as policy server managed through websense enterprise application.	25/02/2012

Samvadak Primary D.C	HCL Infiniti Global Line 2765 XD Server	1	1) Windows Active Directory 2) Windows DNS Server 3) Trend Micro Office scan Server OS: Windows 2003 server	PDC: Configured as a primary domain controller Domain created: sebi_imss.com Core application: Windows Active directory maintains users credentials, authenticate IMSS users login into domain. Main group configured RSA token users. <u>Core secondary application:</u> Windows DNS server.	25/02/2012
Parichayak Secondary D.C	HCL Infiniti Global Line 2765 XD Server	1	1) Windows Active Directory 2) Windows DNS Server OS: Windows 2003 server	BDC: Configured as a backup domain controller. Domain created: sebi_imss.com Core application: <u>Windows Active directory</u> maintains users credentials, authenticate IMSS users login into domain. Main group configured RSA token users <u>Core secondary application: Windows DNS server</u>	25/02/2012
Dootak-Mail Server	HCL Infiniti Global Line 2765 XD Server	1	1) Trend Micro Interscan Message Security Suite 2) Websense Enterprise 3) Cisco Adaptive Security Device Manager (ASDM) 4) Trend Micro Office scan Client.	<u>Core application: Interscan Message Security Suite(IMSS):</u> Acts as SMTP server1)Websense enterprise manager (version installed used for URL filtering on imss clients <u>Cisco ASDM GNU utility</u> for applying configuration to PIX firewall, PIX policies monitoring etc.	25/02/2012

MSS Server	HCL Infiniti Global Line 2765 XD Server	1	1) Checkpoint Smart Dashboard 2) ISS Site protector 3) Net Forensic Agent 4) Trend Micro Office scan Client Administrator OS: Windows 2003 server	Core application: 1) Checkpoint smart dashboard used for firewall rules and policies management, monitor current status firewall cluster, VPN etc. accessed by HCL SOC for monitoring. 2) Core application 2: ISS site protector for IDS management. Net Forensic Agent provides reporting, monitoring integrated with security application i.e. checkpoint and siteprotector. This server is used by NOC/SOC for firewall and IDS report generation.	25/02/2012
RSA Server	HCL Infiniti Global Line 2765 XD Server	1	1) RSA Certificate Utility 2) ISS Site protector Daemon 3) Microsoft SQL Server 4) Trend Micro Office scan Client	Core application: RSA ACE server: authenticate Imss user login through RSA token. Core secondary application: Microsoft SQL server: Database configured event collector of ISS protector domain.	25/02/2012
HARDWARE COMPONENTS - Data sources(NSE,BSE,NSDL,CDSL,MCX)					
Data push in server at NSE	HCL Infiniti Global Line 2765 XD Server	1	OS: Redhat Linux	This server is used by NSE to upload daily transaction master data	25/02/2012
Data push in server at BSE	HCL Infiniti Global Line 2765 XD Server	1	OS: Redhat Linux Database: oracle 9i, sqlplus	This server is used by BSE to upload daily transaction and master data. BSE uploads data into tables. Database configured is oracle 9i. Utility installed sqlplus.	25/02/2012

Data push in server at NSDL	HCL Infiniti Global Line 2765 XD Server	1	OS: Redhat Linux	This server is used by NSDL to upload daily master data	25/02/2012
Data push in server at CDSL	HCL Infiniti Global Line 2765 XD Server	1	OS:Redhat Linux	This server is used by CDSL to upload daily master data	25/02/2012
Data push in server at MCX	IBM Low End Server, rack model	1	OS:Redhat Linux	This server is used by MCX to upload daily master data	----

HARDWARE COMPONENTS - DR site Chennai

Firewall & IDS Server	HCL Infiniti Global Line 2765 XD Server	2	1) ISS Site protector2) Trend Micro Office scan3) Legato Networker4) Remote Administrator 5) Checkpoint Smart console R556) Webtrends Firewall SuiteOS:Windows 2003 server	<p>IDS server: Core application: ISS site protector: used for log collection and monitoring of 2 proventia devices (NIDS).logs are monitored by HCL security operation centre(SOC) Firewall server : Core application: Checkpoint Smart console provides various utilities of checkpoint application. It contains Smart dashboard application which is used for firewall rules and policies management. Other application: webtrend firewall suite: produces firewall and web activity reports that detail security violations. Integrated with security application i.e. checkpoint.</p>	25/02/2012
-----------------------	---	---	--	--	------------

MSS Server	HCL Infiniti Global Line 2765 XD Server	1	<ul style="list-style-type: none"> 1) Checkpoint Smart Dashboard 2) ISS Site protector 3) Net Forensic Agent 4) Trend Micro Office scan Client 5) Legato Networker 6) Remote Administrator OS:Windows 2003 server	<p><u>Core application 1) Checkpoint smart dashboard</u> used for firewall rules and policies management, monitor current status firewall cluster, VPN etc. accessed by HCL SOC for monitoring.</p> <p><u>2)Core application 2: ISS site protector</u> for IDS management Net Forensic Agent: provides reporting, monitoring integrated with security application i.e. checkpoint and siteprotector.This server is used by NOC/SOC for firewall and IDS report generation</p>	25/02/2012
Proxy & URL Filtering server	HCL Infiniti Global Line 2765 XD Server	1	<ul style="list-style-type: none"> 1) Squid 2) InterScan Web Security Suite 3) Websense Policy Server 4) Trend Micro Office scan OS:Windows 2003 server	<p><u>Core application Squid:</u> serves all client for internet connectivity</p> <p><u>Core secondary application: websense:</u> acts as policy server managed through websense enterprise application</p>	25/02/2012
Mail server	HCL Infiniti Global Line 2765 XD Server	1	<ul style="list-style-type: none"> 1) Trend Micro InterScan Message Security Suite 2) Websense Enterprise 3) Cisco Adaptive Security Device Manager (ASDM) 4) Trend Micro Office scan server and client 	<p><u>Core application: Interscan Message Security Suite(IMSS):</u> Acts as SMTP server</p> <p><u>1)Websense enterprise manager:</u> used for URL filtering on imss clients</p> <p><u>Cisco ASDM GNU utility</u> for applying configuration to PIX firewall and policy management</p>	25/02/2012
Domain , BDC & RSA Server	HCL Infiniti Global Line 2765 XD Server	3	<ul style="list-style-type: none"> 1) Windows Active Directory 2) Windows DNS Server 3) Trend Micro Office scan Server 2) ISS Site protector Daemon 3) Microsoft SQL Server 4) Trend Micro Office scan Client 	<p><u>PDC:</u> Configured as a primary domain controller Domain created: sebi_imss.com <u>Core application: Windows Active directory</u> maintains users credentials, authenticate IMSS users login into domain. Main group</p>	25/02/2012

			OS:Windows 2003 server	<p>configured RSA token users.</p> <p><u>Core secondary application: Windows DNS server.</u></p> <p><u>BDC:</u>configured as backup domain controller</p> <p><u>RSA server:</u></p> <p><u>Core application: RSA ACE server:</u> authenticate Imss user login through RSA tokens.</p> <p><u>: Microsoft SQL server:</u> Database configured is event collector of ISS protector domain.</p>	
--	--	--	------------------------	---	--

Network and security equipments at DC site, Data sources (NSE, BSE, NSDL, CDSL, MCX etc) and DR site, Chennai

SNo./ Item	Make & Version	Qty	Software/OS versions installed	Functionality	Warranty till date
NETWORK and SECURITY COMPONENTS					
Firewall & IDS					
CPVP-VCT-U-NG	Check Point Enterprise EBS	1	Software license	Check Point Enterprise Standard Support (EBS) delivers comprehensive, unlimited support.	
SS-CPVP-VCT-U-NG	Software Subscription	3			25/02/2012
CPMP-HVPG-U-NG	Additional VPN-1 Pro Gateways for Load Sharing and High Availability	1			
SS-CPMP-HVPG-U-NG	Software Subscription	3			25/02/2012
EB1639117	Alteon Switched Firewall 5409 Components: Switched Firewall Accelerator 5400, Switched Firewall Director 5009	2	3.5.6.0_R55	Used as external firewall, configured as default gateway towards the internet. One primary firewall -and other secondary firewall. Model ASF 5000 series	
PIX-515E-R-DMZ-BUN	Internal Firewall - Cisco PIX 515 E	1	Cisco PIX Security Appliance Software Version 7.0 (4), Device Manager Version 5.0 (4)	Internal firewall, configured as default gateway for inside network.	25/02/2012
A1204F-1-PB	ISS Proventia A1204	2		NIDS used for intrusion detection purpose.	25/02/2012
P01FW4101 C	Webtrends Firewall Suite v4.1c - Tier 1 Firewall (1 Firewall)	1	Software licenses	This software is used for firewall report generation	25/02/2012
	Websense Enterprise 50 Users with PG1	3	Software licenses.	used for URL filtering on imss clients	

	Trendmicro Neat Suite Enterprise with Scan Mail Exchange for 50 Users	1	Software licenses. Version 7.0	Virus scan	25/02/2012
Routers	CISCO 2651XM	2	IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.3(9c), RELEASE SOFTWARE (fc2)	One router used as internet router, VSNL leased line connectivity terminated on this router and other used as DR-router Mumbai for leased line connectivity to SEBI DR site Chennai	25/02/2012
	WIC-2T	2			
	WIC-1B-S/T	2			
	CAB-SS-V35MT	4			
	S26CK9-12309	2			
	CISCO 3725	2	IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.3(9c), RELEASE SOFTWARE (fc2)	One router used as primary router. <u>Leased lines connections to four locations (NSE, BSE, NSDL, and CDSL)</u> terminated on this router. Other router used as backup router on which <u>ISDN is configured</u> . 28 channels of PRI assigned to NSE, BSE each and 2 channels of PRI link assigned to NSDL, CDSL each.	25/02/2012
	NM-2CE1B	2			
	WIC-2T	3			
	CAB-ACE	2			
	MEM3725-256D-INCL	2			
	CAB-SS-V35MT	5			
	CAB-E1-PRI	4			
	S372CK9-12309	2			
	CISCO2691	4	IOS (tm) C2600 Software (C2600-IK9S-M), Version 12.3(9c), RELEASE SOFTWARE (fc2)	These Routers installed at data sources (NSE, BSE, NSDL, CDSL)	25/02/2012
	CAB-AC	4			
	S269CK9-12309	4			
	NM-1CE1B	4			
	WIC-1T	4			
	CAB-E1-PRI	4			
	MEM2691-256D-INC	4			
	CAB-SS-V35MT	4			
	Cisco 2811	1		Router is installed at MCX	----
Switches					

Layer 3	WS-3750-24TS-E	2	OS: Cisco IOS version 12.2- Layer 3 switch	Used as core inside network. All VLANs are created in this core switch: Connected centrally with L2 switches for VLAN forwarding and connected with external firewall. VLAN info: VLAN1: Management VLAN VLAN10: IMSS users VLAN VLAN20: Domain VLAN VLAN 40:Internet access VLAN VLAN50: Security Management VLAN VLAN60: PIX out VLAN VLAN70External Firewall VLAN VLAN80:MSS VLAN VLAN70 DR router VLAN	25/02/2012
	GLC-SX-MM=	2			
Layer 2	WS-C2950-24	8	OS: Cisco IOS version 12.2	Layer 2 switches. Switches are connected to both layer 3 core switches	25/02/2012
	WS-C2950G-24-E1	4	OS: Cisco IOS version 12.2	Layer 2 Switches are installed at data sources (NSE,BSE,NSDL,CDSL)	25/02/2012
	WS-2950-24	1	OS: Cisco IOS version 12.2	Layer 2 switch is installed at MCX	
Security Solution					
ACESRV-S-00025	RSA Ace Server	1	software license	Authenticate IMSS users login through RSA tokens	25/02/2012
ACEMT-P-S-00025	Maintenance	3			
SD600-6-60-24-250	RSA Secure ID	25		25 RSA tokens configured at DC site, Mumbai	
NETWORK AND SECURITY COMPONENTS - DR Site, Chennai					
5.2.2 Firewall & IDS					
CPVP-VCT-U-NG	Check Point Enterprise EBS	1		Check Point Enterprise Standard Support (EBS) delivers comprehensive, unlimited support.	
SS-CPVP-VCT-U-NG	Software Subscription	3			

EB1639117	Alteon Switched Firewall 5409 Components : Switched Firewall Accelerator 5400, Switched Firewall Director 5009	1	3.5.6.0_R5 5	Used as external firewall, configured as default gateway towards the DC site. One primary firewall	25/02/2012
	n power support	3			25/02/2012
A1204F-1-PB	ISS Proventia A1204	1		NIDS used for intrusion detection purpose	
P01FW4101 C	Webtrends Firewall Suite v4.1c - Tier 1 Firewall (1 Firewall)	1		This software is used for firewall report generation	
PSUFW003E	Software Subscription	3			
	Websense Enterprise 50 Users with PG1	1		used for URL filtering on imss clients	25/02/2012
	Trendmicro Neat Suite Enterprise with Scan Mail Exchange for 50 Users	1		Virus scan	
	Software Subscription	3			
Routers	CISCO 2651XM	1	IOS (tm) C2600	connectivity to DC router, Mumbai	25/02/2012
	WIC-2T	1	Software		
	WIC-1B-S/T	1	(C2600- IK9S-M),		
	CAB-SS-V35MT	2	Version 12.3(9c),		
	S26CK9-12309	1	RELEASE SOFTWARE (fc2)		
	CISCO2691	1	IOS (tm)		25/02/2012

	CAB-AC	1	C2600 Software (C2600-IK9S-M), Version 12.3(9c), RELEASE SOFTWARE (fc2)		
	S269CK9-12309	1			
	NM-1CE1B	1			
	WIC-1T	1			
	CAB-E1-PRI	1			
	MEM2691-256D-INC	1			
	CAB-SS-V35MT	1			
Switches	WS-3750-24TS-E	1	OS: Cisco IOS version 12.2- Layer 3 switch	Used as core inside network. All VLANs are created in this core switch. Connected to layer 2 switches	25/02/2012
Layer 3	GLC-SX-MM=	1			
	WS-C2950-24	2		Layer 2 switches. Switches are connected to layer 3-core switch.	
Layer 2	WS-C2950G-24-EI	3	OS: Cisco IOS version 12.2- Layer 3 switch		25/02/2012
Security Solution	RSA Ace Server	1	software license	Authenticate IMSS users login through RSA tokens	25/02/2012
ACESRV-S-00025	Maintenance	3			
ACEMT-P-S-00025	RSA Secure ID	25		25 RSA tokens configured at DR site, chennai	
SD600-6-60-24-250					

Support services at DC site, Mumbai :(to be continued by HCLT)




S/N	Item	Qty	Purpose	Warranty till date
1	Network Management, device management from HCL Noida Operation Centre(NOC-SOC)	NA	HCL NOC/SOC for network and security devices monitoring.	25/02/2012
2	Resident Engineer at Data Center (3) and DR Site (1)	4	HCL engineers deputed 3 resources at data centre (2 for application support and 1 for network support and 1 network engineer at DR site Chennai.	25/02/2012
3	SMARTS support	NA	SMARTS provides SMARTS application support i.e. SMARTS new version upgrade, maintenance etc	25/02/2012

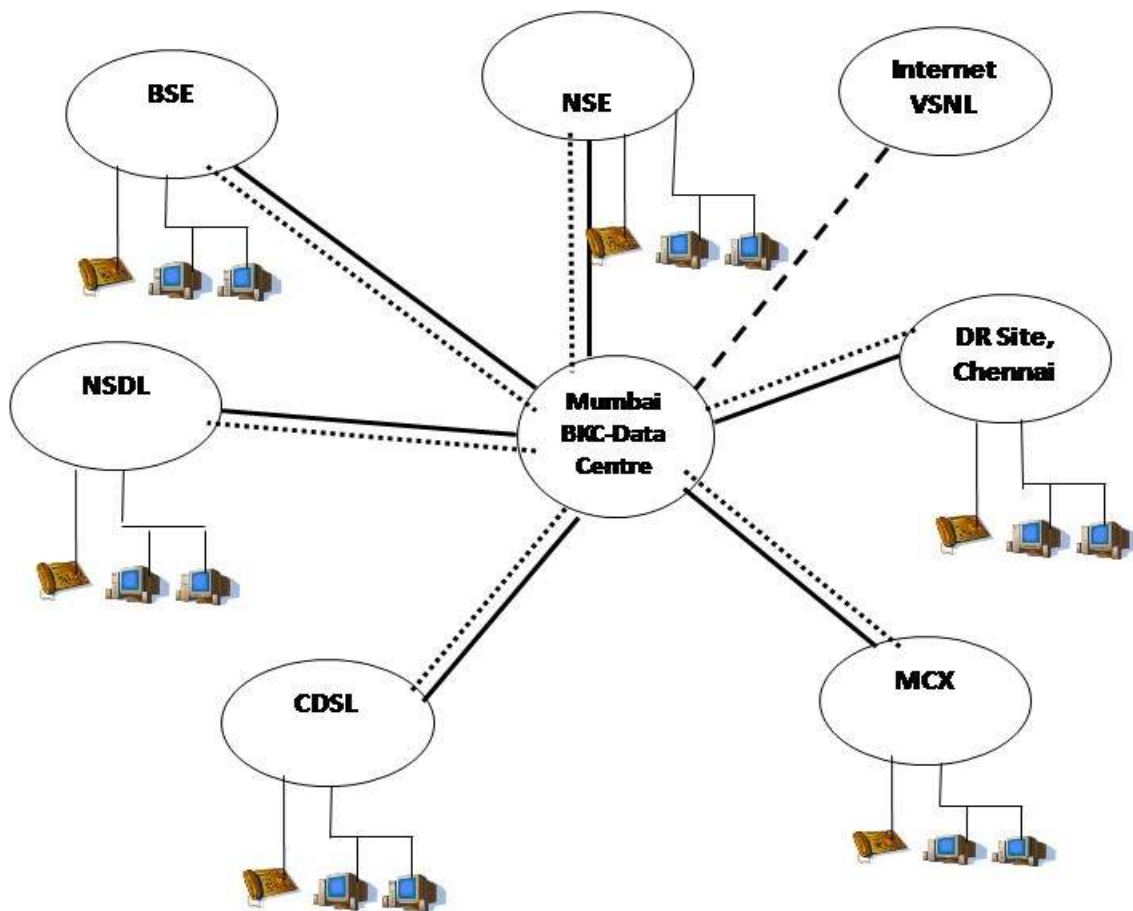
List of system software/application software/applications/utilities installed in existing setup:

1. SMARTS application software
2. OS: Windows 2003 server and Red hat Linux
3. Trend Micro Antivirus
4. Interscan message security suite
5. Interscan web security suite
6. Web sense enterprise manager
7. Web trend firewall suite
8. Cisco ADSM utility
9. Squid
10. ISS site protector
11. Checkpoint SMARTS dashboard
12. RSA ACE server

Annexure D

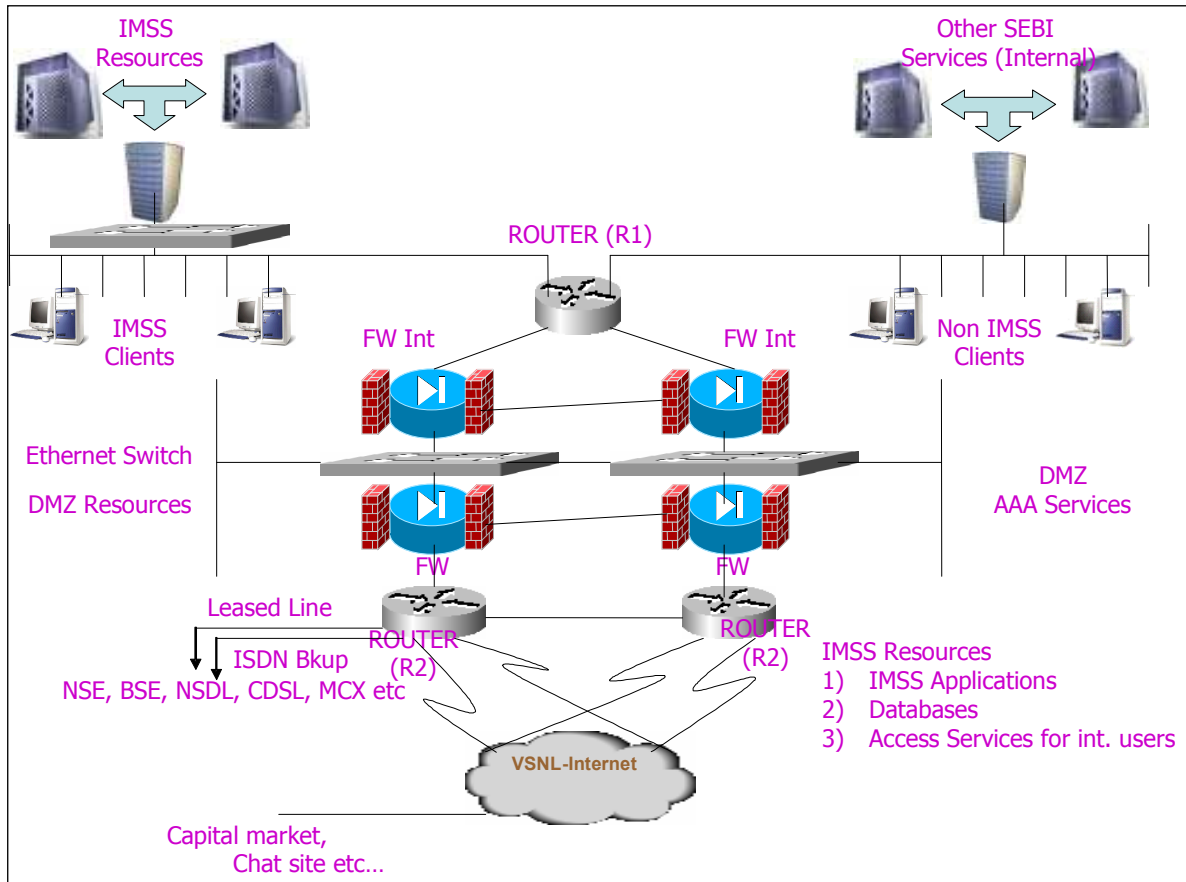
IMSS WAN Connectivity Diagram

-  8 Mbps leased line
-  2 Mbps ISDN backup
-  2 Mbps internet leased line



Network Architecture

The suggested network diagram of IMSS is given below:



Annexure E

Performance Bank Guarantee

Securities and Exchange Board of India
SEBI BHAVAN
Plot No. C4-A, "G" Block
Bandra Kurla Complex, Bandra (E)
Mumbai, India – 400 051

Dear Sirs,

PERFORMANCE BANK GUARANTEE – Supply, Delivery, Installation, Support/Services, Testing, Commissioning, warranty and maintenance for the upgrade of IMSS IT infrastructure to the Securities and Exchange Board of India

WHEREAS

M/s. (name of Bidder), a company registered under the Companies Act, 1956, having its registered and corporate office at (address of the Bidder), (hereinafter referred to as “our constituent”, which expression, unless excluded or repugnant to the context or meaning thereof, includes its successors and assigns), entered into an Agreement dated (hereinafter, referred to as “the said Agreement”) with you (Securities and Exchange Board of India) for supply, delivery, installation, support/services, testing, operationalisation, warranty and maintenance for the upgrade of IMSS IT infrastructure, as detailed in the said Agreement.

We are aware of the fact that in terms of sub-para (...), Section (...), Chapter (...) of the said Agreement, our constituent is required to furnish a Bank Guarantee for an amount Rs..... (in words and figures), being 10% of the Contract Price of Rs. ... (in words and figures), as per the said Agreement, as security against breach/default of the said Agreement by our Constituent.

In consideration of the fact that our constituent is our valued customer and the fact that he has entered into the said Agreement with you, we, (name and address of the bank), have agreed to issue this Performance Bank Guarantee.

▪ Therefore, we (name and address of the bank) hereby unconditionally and irrevocably guarantee you as under :

- I. In the event of our constituent committing any breach/default of the said Agreement, which breach/default has not been rectified within a period of thirty (30) days after receipt of written notice from you, we hereby agree to pay you forthwith on demand such sum/s not exceeding the sum of Rs..... (in words and figures) without any demur.
- II. Notwithstanding anything to the contrary, as contained in the said Agreement, we agree that your decision as to whether our constituent has made any such default/s / breach/es, as aforesaid and the amount or amounts to which you are entitled by reasons thereof, subject to the terms and conditions of the said Agreement, will be

binding on us and we shall not be entitled to ask you to establish your claim or claims under this Performance Bank Guarantee, but will pay the same forthwith on your demand without any protest or demur.

- III. This Performance Bank Guarantee shall continue and hold good till the completion of the warranty period for the 'Total Solution' i.e. (date), subject to the terms and conditions in the said Agreement.
- IV. We bind ourselves to pay the above said amount at any point of time commencing from the date of the said Agreement until the completion of the warranty period for the Total Solution as per said Agreement.
- V. We further agree that the termination of the said Agreement, for reasons solely attributable to our constituent, virtually empowers you to demand for the payment of the above said amount under this guarantee and we have an obligation to honour the same without demur.
- VI. In order to give full effect to the guarantee contained herein, we (name and address of the bank), agree that you shall be entitled to act as if we were your principal debtors in respect of your claims against our constituent. We hereby expressly waive all our rights of surety ship and other rights, if any, which are in any way inconsistent with any of the provisions of this Performance Bank Guarantee.
- VII. We confirm that this Performance Bank Guarantee will cover your claim/s against our constituent made in accordance with this Guarantee from time to time, arising out of or in relation to the said Agreement and in respect of which your claim is lodged with us on or before the date of expiry of this Performance Guarantee, irrespective of your entitlement to other claims, charges, rights and reliefs, as provided in the said Agreement.
- VIII. Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.
- IX. If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you (Securities and Exchange Board of India).
- X. This Performance Bank Guarantee shall not be affected by any change in the constitution of our constituent nor shall it be affected by any change in our constitution or by any amalgamation or absorption thereof or therewith or reconstruction or winding up, but will ensure to the benefit of you and be available to and be enforceable by you.
- XI. Notwithstanding anything contained hereinabove, our liability under this Performance Guarantee is restricted to Rs..... (in words and figures) and shall continue to exist, subject to the terms and conditions contained herein, unless a written claim is lodged on us on or before the afore-said date of expiry of this guarantee.
- XII. We hereby confirm that we have the power/s to issue this Guarantee in your favour under the Memorandum and Articles of Association/ Constitution of our bank and the

undersigned is/are the recipient of authority by express delegation of power/s and has/have full power/s to execute this guarantee under the Power of Attorney issued by the bank in his/their favour.

- 2. We further agree that the exercise of any of your rights against our constituent to enforce or forbear to enforce or any other indulgence or facility, extended to our constituent to carry out the contractual obligations as per the said Agreement, would not release our liability under this guarantee and that your right against us shall remain in full force and effect, notwithstanding any arrangement that may be entered into between you and our constituent, during the entire currency of this guarantee.

Notwithstanding anything contained herein:

- I. Our liability under this Performance Bank Guarantee shall not exceed Rs... (in words and figure) ;
 - II. This Performance Bank Guarantee shall be valid only up to (date, i.e. completion of warranty period for the Total Solution) ; and
 - III. We are liable to pay the guaranteed amount or part thereof under this Performance Bank Guarantee only and only if we receive a written claim or demand on or before (date i.e. completion of the warranty period for the Total Solution).
- This Performance Bank Guarantee must be returned to the bank upon its expiry. If the Performance Bank Guarantee is not received by the bank within the above-mentioned period, subject to the terms and conditions contained herein, it shall be deemed to be automatically cancelled.

Dated this day 2011.

Yours faithfully,

For and on behalf of the Bank,

(Signature)
Designation
(Address of the Bank)

Note :

- a) This guarantee will attract stamp duty as a security bond under Article 54(b) of the Mumbai Stamp Act, 1958.
- b) A duly certified copy of the requisite authority conferred on the official/s to execute the guarantee on behalf of the bank should be annexed to this guarantee for verification and retention thereof as documentary evidence in the matter.

Annexure F

Tender Form-Technical Bid

TENDER FORM

Securities and Exchange Board of
India
SEBI Bhavan, Plot No. C4-A, G-Block,
Bandra Kurla Complex, Bandra (E),
Mumbai - 400051

Gentlemen:

Re: RFP No. SEBI/ TECHNICAL BID

Sub: Supply, Installation, Commissioning and Maintenance of IT infrastructure upgrade of Integrated Market Surveillance System at SEBI

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply, install and commission the **IT infrastructure upgrade for IMSS** and to meet such requirements and provide such services as are set out in the RFP Document.

We attach hereto the Tender/RFP Technical Response as required by the RFP, which constitutes my/our bid.

We undertake, if our Tender/RFP Technical Response is accepted, to adhere to the implementation plan put forward in the Tender/ RFP Technical Response or such adjusted plan as may subsequently be mutually agreed between us and the Securities and Exchange Board of India or its appointed representatives.

If our Tender/RFP Technical Response is accepted, we will obtain a performance bank guarantee in the format given in the Tender Document issued by a scheduled commercial bank in India for a sum equivalent to 10% of the contract sum for the due performance of the contract.

We agree to abide by this Tender/ RFP Technical Response for a period of ONE YEAR from the date fixed for Tender opening and it shall remain binding upon us with full force and virtue, until within this period a formal contract is prepared and executed, this Tender/RFP Technical Response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and will initiate the formation of a separate contract in respect of maintenance and support services after the expiry of the warranty period.

We agree that SEBI is not bound to accept the lowest or any Tender/RFP Technical Response you may receive. We also agree that SEBI reserve the right in absolute sense to reject all or any of the goods /products specified in the Tender/RFP Technical Response without assigning any reason whatsoever.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company /firm/organization and empowered to sign this document as well as such other documents which may be required in this connection.

Dated Day of2011
 this

.....
 (Signature) (In the capacity of)
 Duly authorized to sign the Tender Response for and on behalf of:

(Name and address of Bidding Company)

Seal/Stamp of Tender

Witness name:
 Witness address:

Witness signature:
 Attachments:

- Board resolution delegating signing powers to authorised signatories
- Tender/ RFP Technical Response

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I, certify that I am	Secretary of the	(Name of bidding company)
And that (Name of above company signatory (s))	
Who signed the above Tender is authorized to bind the corporation by authority of its governing body.		
(Seal) (Secretary)	

Annexure G

Tender Form-Commercial Bid

TENDER FORM

Securities and Exchange Board of
India
SEBI Bhavan, Plot No. C4-A, G-Block,
Bandra Kurla Complex, Bandra (E),
Mumbai - 400051

Gentlemen:

Re: RFP No. SEBI/ COMMERCIAL BID

Sub: Supply, Installation, Commissioning and Maintenance of IT infrastructure upgrade of Integrated Market Surveillance System at SEBI

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to supply, install and commission the the **IT infrastructure upgrade for IMSS** and to meet such requirements and provide such services as are set out in the RFP for a total bid price of: _____ **Indian Rupees in words and figures**

We attach hereto the Tender/RFP Commercial Response as required by the RFP, which constitutes my/our bid.

We undertake, if our Tender/RFP Commercial Response is accepted, to adhere to the implementation plan put forward in the Tender/ RFP Technical Response or such adjusted plan as may subsequently be mutually agreed between us and the Securities and Exchange Board of India or its appointed representatives.

If our Tender/RFP Commercial Response is accepted, we will obtain a performance bank guarantee in the format given in the Tender Document issued by a scheduled commercial bank in India for a sum equivalent to 10% of the contract sum for the due performance of the contract.

We agree to abide by this Tender/ RFP Commercial Response for a period of ONE YEAR from the date fixed for Tender opening and it shall remain binding upon us with full force and virtue, until within this period a formal contract is prepared and executed, this Tender/RFP Commercial Response, together with your written acceptance thereof in your notification of award, shall constitute a binding contract between us and will initiate the formation of a separate contract in respect of maintenance and support services after the expiry of the warranty period.

We agree that SEBI is not bound to accept the lowest or any Tender/RFP Commercial Response you may receive. We also agree that SEBI reserve the right in absolute sense to reject all or any of the goods /products specified in the Tender/RFP Commercial Response without assigning any reason whatsoever.

It is hereby confirmed that I/We are entitled to act on behalf of our corporation/company /firm/organization and empowered to sign this document as well as such other documents which may be required in this connection.

Dated Day of2011
this

.....
(Signature) (In the capacity of)
Duly authorised to sign the Tender Response for and on behalf of:

.....
.....
.....
.....

(Name and address of Bidding Company)

Seal/Stamp of Tender

Witness name:

Witness address:

Witness signature:

- Attachments:
- Board resolution delegating signing powers to authorised signatures
 - Tender Commercial Response

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I, certify that I am Secretary
..... of the
..... (Name of bidding company)

And that

.....

.....

(Name of above company signatory (s))

Who signed the above Tender is authorised to bind the corporation by authority of its governing body.

(Seal)

.....

(Secretary)

Annexure H

Bill of materials - IT Infrastructure upgrade

Bidder must ensure that all the items mentioned here correspond to the “Bidders Response Sheet”

SN _o	Item	Make & Version	Quantity	Unit Price (Rs.)	Total Price {Warranty Period 3 Years} (Rs.) (Inclusive of Taxes)	VAT @/Service tax @on “Total price”	AMC 4 th Year (Rs.)	AMC 5 th Year (Rs.)	AMC 6 th Year (Rs.)	Total AMC charges (Rs.)	Service Tax @ for 4 th , 5 th , 6 th year AMC	Net Present Value (NPV)	List Price
1.	Hardware Components												
	Location wise (Data centre, data sources (NSE, BSE, NDSI, CDSL, MCX), DR site, Chennai												
	1.1 Servers												
	1.2 Storage Solution												
	1.3 Data Backup												
	1.5 Any Other												
	Total Hardware												
2.	Network Components												
	Location wise (Data centre, data sources (NSE, BSE, NDSI, CDSL, MCX), DR site, Chennai												
	2.1 Firewall												
	2.2 IDS												
	2.3 Routers												
	2.4 Switches												
	2.5 Management Software												
	2.6 Security Solution												
	2.8 Any Other												
	Total Networking												

SN0	Item	Make & Version	Quantity	Unit Price (Rs.)	Total Price {Warranty Period 3 Years} (Rs.) (Inclusive of Taxes)	VAT @/Service tax @on "Total price"	AMC 4 th Year (Rs.)	AMC 5 th Year (Rs.)	AMC 6 th Year (Rs.)	Total AMC charges (Rs.)	Service Tax @ for 4 th , 5 th , 6 th year AMC	Net Present Value (NPV)	List Price
3.	Software Platform Components												
3.1	Operating system with all utilities, tools & required compilers												
3.2	Databases												
3.3	Middleware (optional)												
3.4	Software/utilities												
3.8	Identity Management (Secure Login)												
3.9	Performance Monitoring & Tuning Tools												
3.11	Any Other Software to meet the Desired Solution												
	Total Software												
6	Ancillary Services												
6.2	Structured Cabling (including the cost of cable etc.)												
	Total Ancillary Services												
7	Project Management												
	Grand Total Price												

Note

1. Every item should be quoted as line item
2. The prices quoted should be inclusive of delivery and installation charges and all Central/ State Government levies, taxes and duties viz., sales tax, excise duty, customs duty, VAT, etc. **excluding octroi**, which will be paid as per the actuals on production of relevant documents.
3. Bidder should specify hardware and software details wherever applicable along with part number, configuration and unit price.
4. Please clearly mention total no. of users and total no. of licenses as necessary for each category of the software.

Annexure I - (Checklist)

CHECKLIST

The bidder shall confirm whether following are submitted in their bid. The bidder shall indicate the page no. at which the details asked below are furnished, otherwise, bid is liable for rejection.

S.No	DETAILS	Submitted (Yes / No)	Page No. at which details are enclosed
1	Technical bid & Commercial bid.		
2	Bids in two parts in English, sealed and superscribed (6 copies – one original and 5 photocopies)		
3	EMD Submitted in Technical Bid		
4	Duly filled and signed forms Annexure F- Covering letter/ Tender Form (Technical Bid) Annexure G - Covering letter/ Tender Form (Commercial Bid) Bidder's Response sheet as per section 4 Checklist Annexure H Bill of Material Annexure E Performance bank Guarantee		
5	Soft Copy of Technical Bid in MS Office-XP (Word/ Excel) or PDF format submitted		
6	Whether the Bid is authenticated by authorized person		
7	Address, contact number and contact person for the Project		
8	All the pages are numbered properly		
9	The latest Annual Report and Audited Balance Sheet, Company details and Capabilities submitted		
10	Joint undertaking with collaborator for satisfactory performance submitted		
11	All pages are authenticated by sign and seal (Full signature to be affixed and not initials). Erasures / Overwriting / Cutting / Corrections authenticated Certification / Undertaking is authenticated.		
12	Whether price quoted are all inclusive except Octroi / Entry tax		
13	Whether replica of price Bid is enclosed in Technical masking price		
14	Whether Taxes and Duties are separately indicated in price bid		