सत्यमेव जयते

सरकार/GOVERNMENT OF INDIA
पोत परिवहन मंत्रालय/MINISTRY OF SHIPPING
नौवहन महानिदेशालय/DIRECTORATE GENERAL OF SHIPPING

टेलीफोन 022 :–25752040 /1/2/ 3	/बिटा बिल्डिंग ,वीं मंजिल9th floor, Beta Building	Tele: 022- 25752040/1/2/3
फैक्स 022 :- 25752029/ 35	आई थिंक टेक्नो कैंपस/I-Think Techno Campus	Fax: 022-25752029/35
ई :मेल-dgship-dgs@nic.in	कांजूर मार्ग /(पूर्व)Kanjur Marg (East)	E-mail: dgship-dgs@nic.in
वेब :www.dgshipping.gov.in	मुंबई/MUMBAI-400 042	Web: www.dgshipping.gov.in

No.E-Gov/New Project(1).2015 Dated : 23.11.2016

CORRIGENDUM TO TENDER NOTICE No. DGS/E-GOV/2016/01

Subject :- Request for Proposal (RFP) for Selection of System integrator for e-Governance solution and transformation of Directorate General of Shipping, Govt. of India.

In continuation of the Tender Notice No.DGS/e-Gov/2016/01 dated 09.11.2016, the last date to receive RFP response submission date has been extended up to **3.00 PM of 09.12.2016** after considering the queries received in response to the Pre-Bid Conference held on 17.11.2016. The interested firms/vendors may submit the tenders as per enclosed Annexure, duly signed and in sealed cover as **"RFP for Selection of System integrator for e-Governance solution and transformation of Directorate General of Shipping, Govt. of India"** to Assistant Director General of Shipping (Admn), Directorate General of Shipping, 9th floor, Beta Building, I-Think Techno Campus, Kanjurmarg (East), Mumbai-400 042" **on or before 3.00 PM on 09.12.2016.** The sealed tenders shall be opened on **09.12.2016 at 4.00 PM** in the office of the Directorate General of Shipping, Kanjurmarg (East), Mumbai.

23/11/2016

[Deependra Singh Bisen]
Asstt. Director General of Shipping

Encl: Annexure (Reply of the queries received)

CORRIGENDUM TO
THE RFP FOR SELECTION OF SI FOR EGOVERNANCE SOLUTION OF DIRECTORATE GENERAL OF SHIPPING

Tender Number: DGS/e-gov/2016/01

Dated: 09/11/2016

CONTENTS

1 Amendment of Clauses

Kindly refer to the table below for amended clauses and sections

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
1.	Volume I	2.1 (II)	8	The tenure of the contract of the successful bidder shall be for a term of five (5) years and Nine (9) months ("the Term")	The tenure of the contract of the successful bidder shall be for a term of five (5) years and Twelve (12) months ("the Term")
2.	Volume I	6.4 (PQ2)	21	Supporting Document: Copy of Audited Annual Balance sheet for last three years ending 31.03.2015 with Certificate from a CA stating Annual Turnover for the last three years In case of: □ Single Bid – Bidder □ Consortium Bid – Lead bidder	Supporting Document: Copy of Audited Annual Balance sheet for last three years ending 31.03.2016 with Certificate from a CA stating Annual Turnover for the last three years In case of: □ Single Bid – Bidder □ Consortium Bid – Lead bidder
3.	Volume I	7.4 (I)	32	DGS reserves the right to negotiate with the bidder(s) whose proposal has been most responsive (the proposal that has been rated best as per calculations done in section 9.1). On this basis the draft contract agreement would be finalized for award & signing.	DGS reserves the right to negotiate with the bidder(s) whose proposal has been most responsive. On this basis the draft contract agreement would be finalized for award & signing.
4.	Volume I	7.5	32	DGS will require the selected bidder to provide a Performance Bank Guarantee, within 15 days from the Notification of award, for a value equivalent to 10% of the total bid value. The Performance Guarantee should be valid for a period of 6 months. The Performance Guarantee shall be kept valid till completion of the project	DGS will require the selected bidder to provide a Performance Bank Guarantee, within 15 days from the Notification of award, for a value equivalent to 10% of the total bid value and should be valid till 6 months post the Contract Period. The Performance Guarantee shall contain a claim period of three months from the last date of validity. In case the Contract Term is extended, the Performance Bank Guarantee should also be extended within

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
				and Warranty period. The Performance Guarantee shall contain a claim period of three months from the last date of validity. The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project and Warranty period. In case the selected bidder fails to submit performance guarantee within the time stipulated, DGS at its discretion may cancel the order placed on the selected bidder without giving any notice. DGS shall invoke the performance guarantee in case the selected Vendor fails to discharge their contractual obligations during the period or DGS incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions	15 days of approval of contract extension and should be valid till 6 months post the Contract Extension Term. The selected bidder shall be responsible for extending the validity date and claim period of the Performance Guarantee as and when it is due on account of non-completion of the project and Warranty period. In case the selected bidder fails to submit performance guarantee within the time stipulated, DGS at its discretion may cancel the order placed on the selected bidder without giving any notice. DGS shall invoke the performance guarantee in case the selected Vendor fails to discharge their contractual obligations during the period or DGS incurs any loss due to Vendor's negligence in carrying out the project implementation as per the agreed terms & conditions
5.	Volume I	9.2 (II) 9.7 (II)	37 42	Clarification	Provisional Go Live will be read as Go Live
6.	Volume I	10.3 (A11.1)	88	SMS Quantity	1,00,00,000

Sr. No .	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
7.	Volume I	6.5 (A.1.2)	24	Prior experience of bidder / any consortium member in implementing **IT solution in Shipping domain as System Integrator*** in last 7 years. **50 marks per project (Maximum 2 projects)**	Prior experience of bidder / any consortium member in implementing **IT solution in Shipping/Transport domain as System Integrator*** in last 7 years. **50 marks per project (Maximum 2 projects)**
8.	Volume II	2.2.1 (VII)	158	The Proposed solution should have a Near Data Centre and Business Continuity and Disaster recovery by taking the RTO and RPO as objective to achieve.	The Proposed solution should have a Data Centre and Business Continuity and Disaster recovery by taking the RTO and RPO and SLA as objective to achieve.
9.	Volume II	2.3 (b)	162	Customers: These are end users who will avail services from DGS. These include port users and estate tenants. Customers may or may not be required to pay for the services they receive.	Customers: These are end users who will avail services from DGS. These include Shipping and Seafarers. Customers may or may not be required to pay for the services they receive
10.	Volume II	3 (b)	163	Handheld devices: refers to hand held devices which are envisaged as a part of the solution, which will be used by operators for access data and providing inputs to the system in case of port and estate operations	Handheld devices: refers to hand held devices which are envisaged as a part of the solution, which will be used by operators for access data and providing inputs to the system in case of shipping and seafarer operations
11.	Volume II	2 (i)	163	Core Operations Group: This is the core operations team which carries out task for port /estate.	Core Operations Group: This is the core operations team which carries out task for shipping/seafareres
12.	Volume II	4 (b)	163	Internal portal: access channel for internal users, interactions related to port and estate operations will be carried out through this portal. Also, access to all internal systems for HR, administration, finance will be provided through	Internal portal: access channel for internal users, interactions related to shipping and seafarer operations will be carried out through this portal. Also, access to all internal systems for HR, Administration etc. will be provided through one portal. Single-

<table>
<tr><th>Sr. No .</th><th>Volume</th><th>Section / Clause</th><th>Page No.</th><th>Original Clause</th><th>Amended Clause</th></tr>
<tr><td></td><td></td><td></td><td></td><td>one portal. Single-sign on facility will be available to eliminate requirement of logging on to different systems</td><td>sign on facility will be available to eliminate requirement of logging on to different systems</td></tr>
<tr><td>13.</td><td>Volume II</td><td>5 (b) 16th Bullet</td><td>171</td><td>Record Management System</td><td>This is deleted.</td></tr>
<tr><td>14.</td><td>Volume II</td><td>6</td><td>171</td><td>This component provides details of various systems central system is expected to interact with. It is assumed that all systems under this assignment will have seamless integration. Interfaces for integration for these systems will have to be looked at by the bidder and integration with these systems as possible after mutual discussion with DGS will have to be arrived at. It is possible that this integration will take place over time and after system goes live. Given below is a minimum indicative list of interfaces which are expected to be designed / built into the proposed system. Bidder may add to the list at the time of requirements gathering phase.
<table>
<tr><td>Sr. No</td><td>Application Name</td></tr>
<tr><td>1</td><td>eParikshа</td></tr>
<tr><td>2</td><td>LRIT</td></tr>
</table></td><td>This component provides details of various systems central system is expected to interact with. It is assumed that all systems under this assignment will have seamless integration. Interfaces for integration for these systems will have to be looked at by the bidder and integration with these systems as possible after mutual discussion with DGS will have to be arrived at. It is possible that this integration will take place over time and after system goes live. Given below is a minimum indicative list of interfaces which are expected to be designed / built into the proposed system. Bidder may add to the list at the time of requirements gathering phase.
<table>
<tr><td>Sr. No</td><td>Application Name</td><td>Integration</td></tr>
<tr><td>1</td><td>eParikshа</td><td>2 way</td></tr>
<tr><td>2</td><td>LRIT</td><td>1 way</td></tr>
<tr><td>3</td><td>eLearning</td><td>2 way</td></tr>
<tr><td>4</td><td>Payment Gateway</td><td>2 way</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Sr. No.</th><th>Volume</th><th>Section / Clause</th><th>Page No.</th><th>Original Clause</th><th>Amended Clause</th></tr>
<tr><td></td><td></td><td></td><td></td><td><table><tr><td>3</td><td>SBI</td></tr><tr><td>4</td><td>eGovernance (if required)</td></tr><tr><td>5</td><td>Payment Gateway</td></tr></table></td><td><table><tr><td>5</td><td>Provident Fund</td><td>Web service based</td></tr><tr><td>6</td><td>Aadhar</td><td>2 way</td></tr><tr><td>7</td><td>SBI (To be decided)</td><td>To be provided by DGS later</td></tr><tr><td>8</td><td>There will be provision to integrate with any external interfaces as required by DGS later.
Ex:
• eImmigration,
• Tab based examination
• e-Office</td><td>To be provided by DGS later</td></tr></table></td></tr>
<tr><td>15.</td><td>Volume II</td><td>1.3.5 (Transitioning – V)</td><td>133</td><td>In addition as users get used to the new system, bidder is expected to help users create ad hoc BI reports, new e-file workflow creation initially. These need to be factored in change management and appropriate training sessions need to be planned and conducted for the same</td><td>In addition as users get used to the new system, bidder is expected to generate MIS reports based on the details submitted in the system. These need to be factored in change management and appropriate training sessions need to be planned and conducted for the same</td></tr>
</table>

Sr. No .	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
16.	Volume II	1.3.2.3 (X)	111	The bidder shall make necessary provisions for management reports, dashboards, business intelligence tools, Mail/SMS gateway, GIS and Data migration in line with the expectations of users provided in the functional requirements and understood during requirement gathering phase	The bidder shall make necessary provisions for management reports, dashboards, Mail/SMS gateway and Data migration in line with the expectations of users provided in the functional requirements and understood during requirement gathering phase
17.	Volume II and Min Tech Specs		117, 157, 158, 160	Clarification	All references to cloud will be read as Cloud ready solution and not cloud implementation
18.	Volume III	21	212	Time is the essence of the Agreement and the delivery dates are binding on the Bidder. In the event of delay or any gross negligence, for causes attributable to the Bidder, in meeting the phase- II Go-live date (Eleven months from the effective date of contract or as proposed by the Bidder), DGS shall be entitled at its option to recover from the Bidder as agreed, liquidated damages, a sum of 0.5% of the Gross Quarterly Payout for each completed week or part thereof subject to a limit of 10% of the estimated Contract value	Time is the essence of the Agreement and the delivery dates are binding on the Bidder. In the event of delay or any gross negligence, for causes attributable to the Bidder, in meeting the implementation phase timelines, DGS shall be entitled at its option to recover from the Bidder as agreed, liquidated damages, a sum of 0.5% of the Gross Quarterly Payout for each completed week or part thereof subject to a limit of 10% of the estimated Contract value.
19.	Volume III	Change Control Process (iii)	231	It is hereby also clarified here that any change of control suggested beyond 20 % of the value of this Project will be beyond the scope of the change control process and will be considered	It is hereby also clarified here that any change of control suggested beyond 20 % of the value of this Project will be beyond the scope of the change control process and will be considered as the subject matter for a separate bid process and

Sr. No .	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
				as the subject matter for a separate bid process and a separate contract. It is hereby clarified that the 20% of the value of the Project as stated in herein above is calculated on the basis of bid value submitted by the Bidder and accepted by DGS or its nominated agencies or as decided and approved by DGS or it Nominated Agencies. For arriving at the cost / rate for change upto 20% of the project value, the payment terms and relevant rates as specified in Annexure D shall apply. Refer to section XX Of Volume XX for estimated contract/project value.	a separate contract. It is hereby clarified that the 20% of the value of the Project as stated in herein above is calculated on the basis of bid value submitted by the Bidder and accepted by DGS or its nominated agencies or as decided and approved by DGS or it Nominated Agencies. For arriving at the cost / rate for change upto 20% of the project value, the payment terms and relevant rates as specified in Annexure D shall apply
20.	Volume III	Annexure (1.3)	254 to 256	Penalty Clauses on Monthly billing in SLA	This should be read as: Penalty on quarterly billing
21.	FRS	Ship Related Processes (OT 2)	358	The system will have login provision for service providers such as labs, FFA/ LSA service stations, ports, etc.	The system will have login provision for service providers such as Bunker suppliers, labs, FFA/ LSA service stations, ports, etc.
22.	FRS	Ship Related Processes (SH1.1 – Technical Clearance)	353	System will create a ship profile based on all the data entered by the user. Certain fields (as per Checklists) are NOT EDITABLE directly by the user in the ship profile. Such fields shall be editable through a separate process called "Amendments to Registry". Other fields can be directly edited by the user. This will form the basis for auto-population when generating letters and certificates from templates.	This is deleted.

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
23.	FRS	Ship Related Processes (SH 2 – Plan Approval)	356		Added to SH 2 System will create a ship profile based on all the data entered by the user. Certain fields (as per checklists) are NOT EDITABLE directly by the user in the ship profile. Such fields shall be editable through a separate process called "Amendments to Registry". Other fields can be directly edited by the user. This will form the basis for auto-population when generating letters and certificates from templates.
24.	FRS	A6 Internal Processing – Processing at Directorate)	303	Addendum to existing clauses	**A6.7** System will have provision to auto-escalate the file to the immediate senior officer if it is unattended by a particular officer
25.	FRS	IN2.1	368	All procurement of goods and services such as such as lease, appointment of contract workers & cleaners, regular maintenance & repair, AMC etc. involving a budget of more than 1 lakh needs to be executed via the tendering process.	Procurement below 1 lakh does not involve the process of tendering. For procurement within 15 thousand to 1 lakh, local purchase committee performs market surveys, calls for quotation and takes approval from administration department. For procurement of goods and services below 15 thousand, only approval from the administration department is taken.
26.	FRS	IN 2.2	368	Procurement below 1 lakh does not involve the process of tendering. For procurement within 15 thousand to 1 lakh, local purchase committee performs market surveys, calls for quotation and takes approval from administration department. For procurement of goods and services below 15 thousand, only approval from the administration department is taken.	All procurement of goods and services such as such as lease, appointment of contract workers & cleaners, regular maintenance & repair, AMC etc. involving a budget of more than 1 lakh needs to be executed via the tendering process.

2 Amended Sections

2.1 Amended Sections of RFP Volume I

A. Section 1.1 – Request for Proposal Datasheet

Sr. No. (2, 7 and 8) in Section 1.1 Volume I shall be read as follows

Sr No.	Bid Information	Details
1.	RFP Issuing Authority	Directorate General of Shipping
2.	RFP reference No and Date	DGS/e-gov/2016/01
3.	Non Refundable Tender Cost	INR 5,000 /-
4.	Earnest Money Deposit (EMD)	INR 20,00,000 /-
5.	Last date and time for submission of queries for clarifications	17/11/2016 by 11:00 am
6.	Date, time and venue of pre-bid conference	17/11/2016 at 12:00 pm Directorate General of Shipping, Government of India, 9th Floor, Beta Building, i-Think Techno campus, Kanjurmarg (East), Mumbai - 400042
7.	Last date, time (deadline) and venue for receipt of proposals in response to RFP notice	09/12//2016 at 3:00 pm Directorate General of Shipping, Government of India, 9th Floor, Beta Building, i-Think Techno campus, Kanjurmarg (East), Mumbai – 400042
8.	Date, time and venue of opening of Proposals received in response to the RFP notice	09/12//2016 at 4:00 pm Directorate General of Shipping, Government of India, 9th Floor, Beta Building, i-Think Techno campus, Kanjurmarg (East), Mumbai – 400042
9.	Place, time and date of Technical Presentations by the bidders	To be communicated later

10.	Place, time and date of opening of Financial Proposals received in response to the RFP notice	To be communicated later
11.	Contact person for queries	Mr. Deependra Singh Bisen <singh.deependra@gov.in>

12.	Method of Selection	The method of selection is Quality and Cost Base Selection (QCBS).
		The weights given to the Technical and Commercial Bids are:
		Technical = 70% and
		Commercial = 30%

B. Section 6.5 – Technical Bid Evaluation

Technical Solution (B) in the section 6.5 of Volume I will be read as follows

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
B	**Technical Solution**	**250**	
B.1	Technical Presentation Marks will be awarded as below: • Approach and Methodology for implementation and maintenance/ Support - 30 Marks • Detailed Project Plan covering scope of work, activities & deliverables as per timelines – 20 Marks • Solution Design meeting all the proposed functionalities – 20 Marks • Risks as seen on this project and their mitigation plan proposed – 20 Marks • Change Management and Training – 10 Marks	150	Presentation to Authorities of DGS (Inclusive of any site visit for designated DGS officials which could be done before or after the presentation). Evaluation of this shall be communicated accordingly to the committee for awarding of marks. The bidders are expected to present their key resources which will be leading the implementation and whose profiles would be evaluated by the evaluation committee

#	PARAMETER	MAX. MARKS	EVIDENCE TO BE SUBMITTED
B.2	Compliance to Functional Requirement Specifications as Listed In Annexure of the Tender	100	Signed Technical Bid

C. Section 9.1 – Project Timelines

Sr. No. (1.5 to 2.1) in Section 9.1 Volume I shall be read as follows

Activity code	Track	Description	Timeline	Acceptance criteria
Phase 1 - Full scale deployment of system across all locations and system stabilization with parallel run				
1.1	PGM	Project kick-off meeting or Agreement signing whichever is earlier	T	D1
1.2	PGM	Submission of project charter	T + 0.5 months	D2
1.3	ASI	Business and system requirements study including interfaces	T + 2 months	D3
1.4	ASI	Solution design including configuration requirements, interface design, etc.	T + 3 months	D4
1.5	ASI	Deployment of complete application software with all modules & required functionalities for user acceptance testing.	T + 9 months	D5
1.6	CDC	Specifications for required Data Centres and Disaster Recovery Centre	T + 2 months	D6
1.7	CDC	Completion of DC and DR	T + 7 months	D7
1.8	NWI	Specifications for networking infrastructure for all sites including DC and DR	T + 2 months	D8
1.9	NWI	Completion of internet connectivity at all locations required for UAT	T + 7 months	D9
1.10	NWI	Completion of network connectivity at all locations required for go-live	T + 10 months	D10
1.11	CSC	Specifications for client side infrastructure as required	T + 2 months	D11
1.12	CSC	Completion of deployment of client infrastructure at all locations required for UAT	T + 7 months	D12
1.13	CSC	Completion of deployment of client infrastructure at all locations required for go-live	T + 10 months	D13
1.14	CMT	Data migration plan	T + 1 months	D14

Activity code	Track	Description	Timeline	Acceptance criteria
1.15	CMT	Submission of change management plan covering training and transitioning requirements	T + 4 months	D15
1.16	CMT	Completion of change management activities including training as required for UAT	T + 7 months	D16
1.17	CMT	Completion of change management activities including training as required for go-live	T + 10 months	D17
1.18	CMT	Completion of data migration	T + 9 months	D18
1.19	IFM	Establishment of IT facilities management system	T + 7 months	D19
1.20	DSD	Procedures and specifications for providing data scanning, digitization and data entry services	T + 1 months	D20
1.21	DSD	Readiness for carrying out data scanning services as per DGS's requirements	T + 2 months	D21
1.22	All	Full scale deployment of the system across all locations	T + 10 months	D22
1.23	All	Successful completion of parallel run with existing system	T + 12 months	D23
1.24	All	Setup of data scanning services for DGS operations	T + 3 months	D24
1.25	All	Certification of SLA monitoring system by third party agency as appointed by DGS	T + 12 months	D25
1.26	All	Stable operations of the system for the 3 months post full scale deployment	T1 = T + 12 months	D26
1.27	ISO	STQC Certification	T + 10	D27
Phase 2 - Operations and maintenance phase				
2.1	ONM	Operations and maintenance of the entire solution for a period of 5 years after stabilization	T1 + 60 months	D28

D. Section 9.2 – Deliverables Schedule

Sr. No. (D5 to D27) in Section 9.2 Volume I shall be read as follows

Deliverables	Deliverable Description	Expected Timelines
D1	Kick-off presentation and/or Duly signed agreement	T
D2	Project charter should cover the following: - Study of scope of work & functional coverage - Detailed project plan - Governance Structure for Project Implementation - Project implementation approach - Work breakdown structure - Delivery schedule - Key milestones - Resource deployment - Change & communication management plan - Change control procedure - Exit management plan	T + 0.5 months
D3	Software Requirements Specifications (SRS) should cover the following: - Detailed requirement capture and analysis - Software requirement - Functional requirement - Interface specifications - Application security requirements - Mapping of FRS & SRS - Requirements sign-off - Identify third party interfaces required along with the type/specifications	T + 2 months
D4	System Design & Configuration report should cover the following: - System Configuration and module wise configuration needs as per the design envisaged - Legacy and Third party System Integration/interface Report and integration of same with the envisaged solutions - Customization Development Plan and Design/development plan of components of functionalities that are not available - High Level Software Design document including Software Architecture design, Logical and Physical Database Design - Low Level Software Design document including Programming Logic, Workflows	T + 3 months
D5	Software Deployment report should cover the following: - Complete Source Code with documentation - Test Plans and Test cases (including Unit Test Plan, System/Integration Test Plan, User Acceptance Test Plan, Security Test Plan, Load Test Plan) - Software Testing Documentation (including details of defects/bugs/errors and their resolution) - User Acceptance Test Cases, Test Data and Test Results, User Acceptance Test Scripts, Unit Test Cases, Integration Test Results/ Cases - System Integration Tests (SIT) including Performance Tests (PT) - Challan of license procurement or verification through online portal of OEM - Periodic data backup and archival post Go-Live. Backup data should be tested for restorability on a quarterly basis.	T + 9 months

Deliverables	Deliverable Description	Expected Timelines
D6	Data centres establishment report should cover the following: - Specifications & Design of DC & DRC - Installation & Commissioning of DC & DRC detailed plan	T + 2 months
D7	Report on DC & DR readiness should cover the following: - Challan of Hardware received from the OEM/ Suppliers	T + 7 months
D8	Network infrastructure establishment report should cover the following: - Comprehensive Network Design - Specifications of network equipment - Network maintenance plan	T + 2 months
D9	Network infrastructure set-up completion for UAT report should cover the following: - Bill of Material (BOM) of network devices & equipment - Challan of Hardware received from the OEM/ Suppliers	T + 7 months
D10	Network infrastructure set-up completion for Go-live report should cover the following: - Bill of Material (BOM) of network devices & equipment - Challan of Hardware received from the OEM/ Suppliers	T + 10 months
D11	Client-side computing establishment report should cover the following: - Detailed specifications of devices to be procured	T + 2 months
D12	Client-side computing set-up completion for UAT report should cover the following: - Devices delivery & installation report - Bill of Material (BOM) of all devices - Challan of Hardware received from the OEM/ Suppliers	T + 7 months
D13	Client-side computing set-up completion for Go-live report should cover the following: - Devices delivery & installation report - Bill of Material (BOM) of all devices - Challan of Hardware received from the OEM/ Suppliers	T + 10 months
D14	Data migration report should cover the following: - Data migration assessment - Migration & transitioning approach - Detailed data migration plan - Scripts required for importing data that has been migrated	T + 1 months
D15	Change Management & Training report should cover the following: - Detailed training plan - Communication plan - Training Materials and Curriculums	T + 4 months
D16	Change Management & Training completion for UAT report should cover the following: - Training session-wise completion reports - Certification from DGS officials confirming successful completion of Change Management & Trainings	T + 7 months
D17	Change Management & Training completion for Go-live report should cover the following: - Training session-wise completion reports - Submission of Final Training Documents - Certification from DGS officials confirming successful completion of Change Management & Trainings	T + 10 months
D18	Data migration completion report should cover the following: - Details of actual data that has been migrated	T + 9 months

Deliverables	Deliverable Description	Expected Timelines
	- Certificate from DGS officials confirming successful completion of data migration	
D19	Establishment of IT facilities management system should cover the following: - Report on Operationalization of Help desk & Call Centre - Standard Operating Procedures and Operations Manuals - Obtaining Relevant Certifications	T + 7 months
D20	Scanning & Digitization procedures & specification report should cover the following: - Requirements gathering of scanning & digitization of DGS - Detailed plan of scanning & digitization - Standard Operating manuals of scanning & digitization	T + 1 months
D21	Scanning & Digitization readiness report should cover the following: - Status of scanning & digitization - Details of completion of activities	T + 2 months
D22	Overall System Deployment report should cover the following: - Deployment sign-off from DGS - User Manuals and System Manuals - Go-Live Certificate indicating readiness for roll-out with trainings - Pending Issues in the system, Dependencies - Updated System Design documents, specifications for every change request - Updated user Manuals, administration manuals, training manuals	T + 10 months
D23	Certification of successful completion of parallel run	T + 12 months
D24	Certification of setup of data scanning services	T + 3 months
D25	Certification of SLA monitoring system by third party agency	T + 12 months
D26	System stabilization report should cover the following: - Report indicating results, observations and action items - UAT Sign-off - Latest source code, application deployment files, configuration files for entire solution - Detailed changes description	T1 = T + 12 months
D27	STQC report and Certificate	T+10
D28	SLA Compliance Reports (Monthly) should cover the following: - Performance Monitoring reports for system - SLA Compliance Reports - Patches/ Upgrades of all components - Incremental updates to solution - Change Requests Managed - Issue/ Problem/ Bugs/Defect Tracker - IT facility management services review report - Scanning & digitization completion & review - On-Going Project Updates - Audit/ Standard Compliance Reports	T1 + 60 months

E. Section 10.3 – Comp 1: Summary of Commercial Proposal

Table A9 in Section 10.3 Volume I shall be read as follows

Sub Total (A1.3+ A9.1.1)	Sub Total (A2.3+ A9.1.2)	Sub Total (A3.3+ A9.1.3)	Sub Total A4	Sub Total (A5.3+ A9.1.4)	Sub Total A6	Sub Total (A7.3+ A9.1.5)	Sub Total (A8.3+ A9.1.6)	Total Value (A9.2)	Total A9= (A9.2 + Tax amount)

2.2 Indicative Bill of Material

The following section provides a minimum indicative list of bill of material for the project. Bidder shall make its own independent assessment to meet the desired service levels as stated in Volume III of the RFP. However, the final bill of material will not be lesser than what has been provided in this section.

2.2.1 Central System

DC & DR Bill of Material				
S No.	**Equipment / Parts**	**DC**	**DR**	**UAT**
1	Edge Server	2	1	1
2	Web Server	4	2	1
3	Database Server	2	2	1
4	Application Server	2	2	0
5	Directory Server	1	1	0
7	Reporting Server	1	1	0
8	Log Server	1	1	0
9	Integration Server	1	1	0
10	Storage Manager Server	1	1	0
11	EMS Server	1	1	0
12	Helpdesk Server	1	1	0
13	Backup and Archival Server	1	1	0
14	Staging Server	1	1	0
15	Storage Area Network (SAN) Array – 10 TB	1	1	0
16	Tape Library – 2 Slot/Drive (Tape 20 nos x 1 TB)	1	1	0
17	Core Router	1	1	0
18	Primary Firewall	1	1	0

DC & DR Bill of Material				
S No.	**Equipment / Parts**	**DC**	**DR**	**UAT**
19	Internal Firewall	1	1	0
20	Edge Router	1	1	0
21	Intrusion Prevention System (IPS)	2	1	0
22	Core & Distribution Switch L3 48 Ports Managed	2	1	0
23	Server Farm L3 Switch 24 Ports Managed	2	1	0
28	SLA Software	1	1	1

2.2.2 DGS, Head Office, Mumbai

Central Office Bill of Material (1 Location)			
#	**Equipment / Parts**	**Quantity per Location**	**Total Quantity**
1	Workstations	120	120
2	Printers	10	10
3	Scanners	5	5
4	LAN Unmanaged Switch L2 24 Ports	5	5
5	UPS with 60 minutes Battery Backup	1	1
6	Router	1	1
7	Laptops	30	30

2.2.3 DGS MMD offices

Regional Office Bill of Material (14 Locations)		
#	**Equipment / Parts**	**Total Quantity**
1	Workstation	215

Regional Office Bill of Material (14 Locations)		
#	**Equipment / Parts**	**Total Quantity**
2	Router	14
3	LAN Unmanaged Switch 8 Ports	14
4	UPS with 60 minutes Battery Backup	14
5	Printers	25
6	Scanners	12
7	Laptops	35

2.2.4 DGS Other offices

Other Office Bill of Material (13 locations)		
S No.	**Equipment / Parts**	**Total Quantity**
1	Workstation	65 (approx.)
2	Router	13 (approx.)
3	LAN Unmanaged Switch 8 Ports	13 (approx.)
4	UPS with 60 minutes Battery Backup	13 (approx.)
5	Printers	15 (approx.)
6	Scanners	8 (approx.)
7	Laptops	35 (approx.)

2.3 Abbreviations

Sr No.	Abbreviation	Full Form
1.	AMC	Annual Maintenance Contract
2.	AOA	Article of Agreement
3.	APAC	Automated Program Analysis for Cybersecurity
4.	APAR	Annual Performance Appraisal Report
5.	API	Application Program Interface
6.	ASC	Annual Service Contract
7.	ASI	Application Software and Interfaces
8.	ATOM	Any Transport over MPLS
9.	BE	Bachelor of Engineering
10.	BOM	Bill of Material
11.	BOQ	Bill of Quantity
12.	CAD	Computer Aided design
13.	CCA	Controller of Certifying authority
14.	CCB	Change Control Board
15.	CCN	Change Control Note
16.	CDC	Continuous Discharge certificates
17.	CGHS	Central Government Health Scheme
18.	CMS	Content Management System
19.	CMT	Change management, Migration and transitioning
20.	COC	Certificate of Compliance
21.	COE	Certificate of Endorsement
22.	COP	Certificate of Proficiency
23.	COS	Certificate of Service
24.	COTS	Commercial off-the-shelf
25.	CPWD	Central Public Works Department
26.	CS	Commercial Score
27.	CSC	Client Side Computing
28.	CSE	Customer Service Executive
29.	CVO	Chief Vigilance Officer
30.	CVS	Concurrent Versions System
31.	DBA	Database Administrator
32.	DC	Data Centre
33.	DD	Demand Draft
34.	DDOS	Distributed Denial of Service
35.	DGS	Directorate General of Shipping
36.	DHTML	Dynamic Hyper Text Markup Language
37.	DMZ	Demilitarized Zone
38.	DOC	Document Of Compliance
39.	DOM	Document object Model
40.	DPC	Department promotion committee
41.	DR	Disaster Recovery
42.	DRC	Disaster Recovery Centre
43.	DSC	Digitally Signed Certificates
44.	DSD	Data Scanning and Digitization
45.	EMD	Earnest Money Deposit
46.	EMS	Enterprise management system
47.	FOBOT	Fibre optic break out tray
48.	FRS	Functional Requirement Specification

Sr No.	Abbreviation	Full Form
49.	FSI	Flag State Inspection
50.	FSICS	Flag State Inspection Computerised System
51.	GMDSS	Global Maritime Distress and Safety System
52.	GOI	Government of India
53.	HR	Human Resource
54.	HRMS	Human Resource Management System
55.	HTML	Hypertext Markup Language
56.	HTTPS	Hypertext Transfer Protocol Secure
57.	ICT	Information Communications Technology
58.	IFM	IT facilities management
59.	IIITB	International Institute of Information Technology, Bangalore
60.	IME	Institute of Marine Engineer
61.	IMO	International Maritime Organization
62.	IMU	Indian Maritime University
63.	INDOS	Indian National Database Of Seafarers
64.	IOMOU	Indian Ocean Memorandum of Understanding
65.	IPR	Intellectual Property Rights
66.	ISM	International Safety Management
67.	ISO	ISO policies
68.	IT	Information Technology
69.	ITIL	Information technology Infrastructure Library
70.	IVR	Interactive Voice Response
71.	KPI	Key Performance Indicator
72.	LLP Act	Limited Liability Partnership Act
73.	LRIT	Long Range Identification Tracking
74.	MACP	Modified Assured Career Progression
75.	MathML	Mathematical Markup Language
76.	MBA	Master of Business Administration
77.	MCA	Master of Computer Application
78.	MDM	Mobile Device Management
79.	MHTML	MIME (Multipurpose Internet Mail Extensions) Hypertext Markup Language
80.	MIS	Management Information System
81.	MMD	Mercantile Marine Department
82.	MMSI	Maritime Mobile Service Identity
83.	MOU	Memorandum of Understanding
84.	MPLS	Multiprotocol label switching
85.	MS Act	Merchant Shipping Act
86.	MSA	Master Service Agreement
87.	MSL	Merchant Shipping Law
88.	MSP	Managed Service Provider
89.	MSV	mechanized sailing vessels
90.	MTI	Maritime Training Institute
91.	MTO	Multimodal Transport Operators
92.	NDA	Non-Disclosure Agreement
93.	NSIC	National Small Industries Corporation
94.	NWB	National welfare board
95.	NWI	Networking infrastructure

Sr No.	Abbreviation	Full Form
96.	ODBC	Open Database Connectivity
97.	ODF	Open Document Format
98.	OECD	Organisation for Economic Co-operation and Development
99.	OEM	Original Equipment Manufacturer
100.	OFC	Optical Fibre Cable
101.	OMA	Open Mobile Alliance
102.	ONM	Operations and maintenance
103.	OTDR	Optical Time Domain Reflectometer
104.	OWASP	Open web application security project
105.	PBG	Performance Bank Guarantee
106.	PDC	Primary Data Centre
107.	PGM	Project governance and management
108.	PIU	Project Implementation Unit
109.	PKI	Public Key Infrastructure
110.	PMO	Project Management Office
111.	PO	Principal Officer
112.	POP	Point of presence
113.	POS	Point of Sale
114.	PQ	Pre-Qualification Criteria
115.	PSC	Port State Control
116.	PSU	Public Sector Undertaking
117.	PT	Performance Testing
118.	QCBS	Quality and Cost Base Selection
119.	REST	Representational State Transfer
120.	RFP	Request for proposal
121.	RO (S)	Regional Office (Sails)
122.	RPO	Recovery Point Objective
123.	RPS	Recruitment and Placement Agencies for Seafarers
124.	RR	Recruitment Rule
125.	RSS	Rich Site Summary
126.	RTF	Rich Text Format
127.	RTI	Right to Information
128.	RTO	Recovery Time Objective
129.	SC	Subscriber Connector
130.	SDLC	System Development Life cycle
131.	SEO	Seamen Employment Office
132.	SI	System Integrator
133.	SIC	Surveyor in Charge
134.	SIT	System Integration Testing
135.	SLA	Service Level Agreement
136.	SM	Shipping Master
137.	SMC	Safety Management Certificate
138.	SMLC	System Maintenance Life cycle
139.	SMS	Safety Management System
140.	SOA	Service Oriented Architecture
141.	SOAP	Simple Object Access Protocol
142.	SOLAS	Safety Of Life At Sea

Sr No.	Abbreviation	Full Form
143.	SPFO	Seamen's Provident Fund Organization
144.	SRS	Software Requirement Specifications
145.	SSC	Staff selection Committee
146.	SSDG	State e-Governance Service Delivery Gateway
147.	STCW	Standard Of Training Certificate And Watch Keeping Code
148.	STQC	Standardization Testing and Quality Certification
149.	SVG	Scalable Vector Graphics
150.	SWFS	Seamen's Welfare Fund Society
151.	SWO	Seamen's Welfare office
152.	TAT	Turnaround time
153.	TCO	Total Cost of Ownership
154.	TS	Technical Score
155.	UAT	User Acceptance Testing
156.	UDDI	Universal Description, Discovery, and Integration
157.	UPSC	Union Public Service Commission
158.	URI	Uniform Resource Identifier
159.	URN	Uniform Resource Name
160.	UTP	Unshielded Twisted Pair
161.	VCC	Vigilance Clearance Certificate
162.	VLAN	Virtual Local Area Network
163.	VM Attack	Virtual Machine Attack
164.	VPN	Virtual Private Network
165.	W3C	World Wide Web Consortium
166.	WCAG	Web Content Accessibility Guidelines
167.	WebDAV	World Wide Web Distributed Authoring and Versioning
168.	WSDL	Web Services Description Language
169.	WSRP	Web Services for Remote Portlets
170.	XHTML	Extensible Hypertext Markup Language
171.	XML	Extensible Markup Language
172.	XPS	XML (Extensible Markup Language) Paper Specification
173.	XSLT	Extensible Stylesheet Language Transformations

2.4 Minimum Technical Specifications

#	**Components**
1	Desktop
2	Laptop
3	Managed Access Switch
4	Data Center hosting specifications (Servers, Storage etc)
5	Enterprise Management System (EMS)
6	Backup and Archival
7	Multi-function Printer & Scanner
8	Intranet Firewall
9	Internet Firewall
10	Intrusion Prevention System
11	Optical Fibre Cable (OFC)
12	Intranet Router
13	Internet Router
14	Core Switch

#	Nature of Requirement	Minimum Requirement Description for Desktop
1	CPU	Intel or AMD
2	Processor	Intel Pentium Core i7 or Higher and for AMD A6 6400 CPU or better
3	CPU Speed	Minimum 3 GHz or higher
4	Chipset	Intel H81 or Higher for A75 Chipset or higher
5	Cache Memory	Minimum 3 MB or higher
6	Memory	8 GB DDR3 RAM Min. 667MHz Upgradable up to 16GB
7	HDD	1TB @ HDD 7200 RPM
8	HDD Controller	Integrated dual port SATA-II controller
9	Operating System	Preloaded with latest windows 8.1 or higher professional 64 bit OS which can be down gradable to Win 7 Professional 64 bit on requirement.
10	Monitor	Minimum 18.5" or higher wide monitor with TCO5 certification: 1366 X 768
11	Keyboard (Bilingual , Hindi and English)	Min. 104 Keys OEM Mechanical Key Board or TVSE Gold or Equivalent
12	Mouse	Two Button Optical Scroll Mouse
13	Optical Drive	22X DVD writer or higher and the corresponding software
14	Cabinet	Micro-ATX/ Desktop
15	Ports	Min. 6 USB (2 In front), 1 Serial, 1 Parallel, PS/2 (For Keyboard & Mouse)
16	Certification	TCO 05 certified Monitor; Energy star 5.0 or above/ BEEstar certified; 80plus certified power supply; The Restriction on Hazardous Substance Directives (RoHS) for environment safety.
17	Anti-Virus	Preloaded antivirus along with patches and updates for 5 years.
18	Warranty	Comprehensive 5 years onsite warranty

#	Nature of Requirement	Minimum Requirement Description for Laptop
1	Processor	Intel Pentium Core i5 or Equivalent
2	Speed	Minimum 3 GHz or higher
3	Memory	4 GB DDR3 RAM Min. 667MHz Upgradable up to 8GB
4	HDD	250 GB @ HDD 7200 RPM
5	HDD Controller	Integrated dual port SATA-II controller
6	Operating System	Preloaded with latest windows 8.1 or higher professional 64 bit OS which can be down gradable to Win 7 Professional 64 bit on requirement.
7	Display	Minimum 12” or higher wide display with TCO5 certification: 1366 X 768 HD LED Anti-Glare Display
8	Keyboard (Bilingual , Hindi and English)	Min. 104 Keys OEM Mechanical Key Board or TVSE Gold or Equivalent
9	Mouse	Two Button Optical Scroll Wireless Mouse
10	Ports	Min. 3 USB 3.0
11	Anti-Virus	Preloaded antivirus along with patches and updates for 5 years.
12	Warranty	Comprehensive 5 years onsite warranty
13	Networking	Ethernet Port: 1, Ethernet Type: 10/100/ 1000, WiFi Type: 802.11b/g/ n, LAN connectivity
14	Standard Battery	Upto 9 hours back-up, 6 cell including Charger
15	Additional features	Built-in HD Camera, Microphone, Digital Media Reader slot, Light weight, Bluetooth, Speakers, Touchpad with Track Point

#	Nature of Requirement	Minimum Requirement Description for Managed Access Switch
1	Switch Architecture and Performance	Switch should have 24 Nos. 10/100/1000Base-TX auto-sensing plus 4x1G SFP uplinks.
2	Switch Architecture and Performance	Should support stacking using dedicated stacking ports with up to 80Gbps throughput
3	Switch Architecture and Performance	Switch should support link aggregation across multiple switches in a stack.
4	Switch Architecture and Performance	Should support stacking of minimum of eight switches
5	Switch Architecture and Performance	Switch should have non-blocking wire-speed architecture.
6	Switch Architecture and Performance	Switch should support IPv4 and IPv6 from day One
7	Switch Architecture and Performance	Switch should have non-blocking switching fabric of minimum 56 Gbps or more
8	Switch Architecture and Performance	Switch should have Forwarding rate of minimum 41 Mpps.
9	Layer 2 Features	IEEE 802.1Q VLAN tagging.
10	Layer 2 Features	802. 1Q VLAN on all ports with support for minimum 255 active VLANs and 4k VLAN ids
11	Layer 2 Features	Support for minimum 8k MAC addresses
12	Layer 2 Features	Spanning Tree Protocol as per IEEE 802.1d
13	Layer 2 Features	Multiple Spanning-Tree Protocol as per IEEE 802.1s
14	Layer 2 Features	Rapid Spanning-Tree Protocol as per IEEE 802.1w
15	Layer 2 Features	Self-learning of unicast & multicast MAC addresses and associated VLANs
16	Layer 2 Features	Jumbo frames up to 9000 bytes
17	Layer 2 Features	Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.
18	Layer 2 Features	Port mirroring functionality for measurements using a network analyzer.
19	Layer 2 Features	Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping.
20	Quality of Service (QoS) Features	Switch should support IGMP v1/v2/v3 as well as IGMP v1/v2/v3 snooping.
21	Quality of Service (QoS) Features	Switch should support DiffServ as per RFC 2474/RFC 2475.
22	Quality of Service (QoS) Features	Switch should support four queues per port.
23	Quality of Service (QoS) Features	Switch should support QoS configuration on per switch port basis.
24	Quality of Service (QoS) Features	Switch should support classification and marking based on IP Type of Service (TOS) and DSCP.
25	Quality of Service (QoS) Features	Switch should provide traffic shaping and rate limiting features (for egress as well as ingress traffic) for specified Host, network, Applications etc.
26	Quality of Service (QoS) Features	Strict priority queuing guarantees that the highest-priority packets are serviced ahead of all other traffic.
27	Security Features	Switch should support MAC address based filters / access control lists (ACLs) on all switch ports.
28	Security Features	Switch should support Port as well as VLAN based Filters / ACLs.
29	Security Features	Switch should support RADIUS and TACACS+ for access restriction and authentication.
30	Security Features	Secure Shell (SSH) Protocol, HTTP and DoS protection
31	Security Features	IP Route Filtering, ARP spoofing, DHCP snooping etc.
32	Security Features	Should support DHCP snooping, DHCP Option 82, Dynamic ARP Inspection (DAI)
33	Security Features	Should support a mechanism to shut down Spanning Tree Protocol Port Fast-enabled interfaces when BPDUs are received to avoid accidental topology loops.

34	Security Features	Should support a mechanism to prevent edge devices not in the network administrator's control from becoming Spanning Tree Protocol root nodes.
35	Security Features	Switch should support static ARP, Proxy ARP, UDP forwarding and IP source guard.
36	Security Features	Switch should Support Ipv6 First hop Security with the following functions: IPv6 snooping, IPv6 FHS binding, neighbor discovery protocol (NDP) address gleaning, IPv6 data address gleaning, IPv6 dynamic host configuration protocol (DHCP) address gleaning, IPv6 device tracking, neighbor discovery (ND) Inspection, IPv6 DHCP guard, IPv6 router advertisement (RA) guard
37	Management, Easy-to-Use Deployment and Control Features	Switch should have a console port with RS-232 Interface for configuration and diagnostic purposes.
38	Management, Easy-to-Use Deployment and Control Features	Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3.
39	Management, Easy-to-Use Deployment and Control Features	Switch should support all the standard MIBs (MIB-I & II).
40	Management, Easy-to-Use Deployment and Control Features	Switch should support TELNET and SSH Version-2 for Command Line Management.
41	Management, Easy-to-Use Deployment and Control Features	Switch should support 4 groups of embedded RMON (history, statistics, alarm and events).
42	Management, Easy-to-Use Deployment and Control Features	Switch should support system and event logging functions as well as forwarding of these logs to multiple syslog servers.
43	Management, Easy-to-Use Deployment and Control Features	Switch should support on-line software reconfiguration to implement changes without rebooting. Any changes in the configuration of switches related to Layer-2 & 3 functions, VLAN, STP, Security, QoS should not require rebooting of the switch.
44	Management, Easy-to-Use Deployment and Control Features	Support for Automatic Quality of Service for easy configuration of QoS features for critical applications.
45	Management, Easy-to-Use Deployment and Control Features	Support for Unidirectional Link Detection Protocol (UDLD) to detect unidirectional links caused by incorrect fiber-optic wiring or port faults and disable on fiber-optic interfaces
46	Management, Easy-to-Use Deployment and Control Features	Switch should have comprehensive debugging features required for software & hardware fault diagnosis.
47	Management, Easy-to-Use Deployment and Control Features	Layer 2/Layer 3 trace route eases troubleshooting or equivalent feature supporting IEEE 802.1 AG, IEEE 802.3 AH identifying the physical path that a packet takes from source to destination.
48	Management, Easy-to-Use Deployment and Control Features	Should support DHCP Server feature to enable a convenient deployment option for the assignment of IP addresses in networks that do
49	Management, Easy-to-Use Deployment and Control Features	not have without a dedicated DHCP server.
50	Management, Easy-to-Use Deployment and Control Features	Switch should support Multiple privilege levels to provide different levels of access.
51	Management, Easy-to-Use Deployment and Control Features	Switch should support NTP (Network Time Protocol)
52	Management, Easy-to-Use Deployment and Control Features	Switch should support FTP/ TFTP

53	Standards	RoHS Compliant.
54	Standards	IEEE 802.1x support.
55	Standards	IEEE 802.3x full duplex on 10BASE-T and 100BASE-TX ports.
56	Standards	IEEE 802.1D Spanning-Tree Protocol.
57	Standards	IEEE 802.1p class-of-service (CoS) prioritization.
58	Standards	IEEE 802.1Q VLAN.
59	Standards	IEEE 802.3u 10 BaseT / 100 Base Tx /1000 Base Tx.
60	Compliance	The switch should be IPV6 complaint

#	Solution Objective and Minimum Requirements for Servers
1	The servers should be sized by BIDDER independently considering the business requirements and workload details provided in this document.
2	BIDDER should provision the server infrastructure required for the solutions that would be deployed at the DC and DR sites.
3	The infrastructure at the above sites will require different types of servers. BIDDER is responsible for understanding the niche requirements of all applications and provide servers as required to make the proposed solution complete.
4	The servers should be sized such that it would not utilize more than 70% of its resources (CPU and I/O) in normal course (with an exception to the batch processes). The utilization should not exceed 70% for a sustained period of more than 15 minutes (with an exception to the batch processes).
5	The proposed servers should be rack / blade optimized with scalability for additional CPU, Memory and I/O.
6	The proposed servers should have adequate number of CPUs with latest clock speed and cache.
7	Servers should be of latest generation and highest clock speed at the time of supply.
8	The servers should be based on Symmetrical Multiprocessing (‘SMP’) architecture.
9	Each server should be populated with adequate number of internal disks.
10	The disks should be Hot Swappable and should be proposed in hardware mirrored configuration using an Ultra 320 SCSI/FC-AL/SAS Controller with Hardware RAID Level 0 and 1.
11	Each server should be populated with adequate number of Gigabit full-duplex Ethernet controllers for LAN connectivity. The Ethernet controllers should be configured for dual homing and they should provide adequate throughput to each switch based on the solution deployed on the server.
12	The servers that need connectivity to SAN should be populated with adequate number of Fiber Channel Host Bus Adaptors (‘HBA’) in redundant mode.
13	The servers should be proposed with redundant and hot swappable power supplies.
14	All the servers, except the Server for backup, should be populated with read-only drive, capable of reading all types of CD / DVD.
15	Except the server for backup, none of the servers should be populated with any writeable media.
16	BIDDER should propose rack mounted KVM switch based consoles within the SDC for monitoring and managing the servers. Every server should not be provisioned with monitor, keyboard and mouse individually. It is envisaged that the servers would also be monitored remotely using the EMS solution.
17	BIDDER should provide requisite licenses for all the software required for the respective servers including, but not limited to, Operating System, respective software database and application, etc.
18	BIDDER should propose servers after taking into account the design consideration.

#	Minimum Requirement for Web Server(s)
1	The Web Servers will be mainly used for running the proposed HTTP Server to manage connections of user sessions.
2	BIDDER should provide requisite open source software for the web server including, but not limited to, Operating System, etc.
3	Enterprise web services - package and deploy components as Web services and their clients in a standard way
4	Support for Web Services Notification, which enables Web Service applications to utilize the ‘Publish and Subscribe’ messaging pattern
5	Support for WSDL 1.1
6	Support for WS Interoperability Basic security profile, to provide transport-neutral mechanisms to address WS and to facilitate end-to-end addressing
7	Support for WS Business Agreement
8	Support for UDDI 3.0
9	Support for SOAP 1.2
10	Support for HTTP 1.1 support for Web service server & client
11	Support for REST based services
12	Ability to consume web services from external systems (including .NET)
13	Support for TEXT / XML Digital Signature & Encryption
14	Web Services Management Capabilities (Provisioning, Encryption, Digital Signature, Key Exchanges, Auditing)
15	Support for Asynchronous Web Services
16	WS-Security 1.1
17	Web services TEXT / XML compression (gzip, etc.)
18	Support for caching of Web Services responses
19	Support for edge serving of Web Services
20	Support for Web Services message security APIs

#	Minimum Requirements for Application Server(s)
1	The Application Servers will be mainly used for running the business logic of the core application.
2	The Application Servers should be sized by BIDDER independently.
3	BIDDER should provide requisite licenses for all the system software required for the application server including, but not limited to, Operating System, Application Server Software, etc.

#	Chassis Specification for All Servers
1	Single blade chassis should accommodate minimum 6 (Quad-Processor)/8 (Dual Processor) or higher hot pluggable blades.
2	6U to 12U Rack-mountable
3	Dual network connectivity for each blade server for redundancy should be provided. Backplane should be completely passive device. If it is active, dual backplane should be provided for redundancy
4	Should accommodate Intel, AMD, RISC / EPIC Processor based Blade Servers for future applications
5	Same chassis should support dual CPU and Quad CPU blades
6	Should have the capability for installing industry standard flavours of Linux / Unix Operating Environments
7	Single console for all blades in the enclosure or KVM Module
8	DVD ROM can be internal or external, which can be shared by all the blades allowing remote installation of S/W and OS
9	Should support the external storage
10	Minimum 2 external USB connections functionality
11	Two hot-plug, redundant 1Gbps Ethernet module with minimum 10 ports (cumulative), which enable connectivity to Ethernet via switch. Switch should be (Internal/external) having Layer 3 functionality - routing, filtering, traffic queuing etc.
12	Two hot-plugs, redundant >=4 Gbps Fiber Channel for connectivity to the external Fiber channel Switch and ultimately to the storage device
13	Power Supplies:
	- Hot Swap redundant power supplies to be provided.
	- Power supplies should have N+N. All Power Supplies modules should be populated in the chassis.
14	Hot Swappable and redundant Cooling Unit
15	LED / LCD Alerts/ indication on Hard disk drives, processors, blowers, memory
16	Management
	- Systems Management and deployment tools to aid in Blade Server configuration and OS deployment,
	- Remote management capabilities through internet browser
	- It should provide Secure Sockets Layer (SSL) 128 bit encryption and Secure Shell (SSH) Version 2 and support VPN for secure access over internet.
	- Ability to measure power historically and cap power for servers or group of servers for optimum power usage
	- Ability to monitor performance of servers over time
	- Blade enclosure should have display console for local management like trouble shooting, configuration, system status/health display
17	Built in KVM switch or Virtual KVM feature over IP
18	Dedicated management network port should have separate path for management
19	Support heterogeneous environment: Intel, AMD, Xeon and RISC/EPIC CPU blades must be in same chassis with scope to run Open source OS, Windows 2012 Server, Red Hat Linux / 64 Bit UNIX, Suse Linux / 64 Bit UNIX / etc.

#	Nature of Requirement	Minimum Requirements for Database Server(s)
	General	
1		The server will be used to store the data that is necessary for the functioning of solution.
2		The server should have ability to process mixed transaction loads (batch and online) and have the ability to dynamically configure processor power according to workload requirements.
3		The server should be configured in active-active high availability mode with cluster at all requisite levels such as OS, database
4		BIDDER should provide open source software for the database server including, but not limited to, Operating System, Database, etc.
5		The model of the server proposed should have capability for field expansion for minimum 25% additional Processors and minimum 40% additional Memory and 40% additional I/O slots in each node over and above the relative capacity for the 5th year as demonstrated during commissioning.
6		The server should be sized for the load the end of 5th year, but the server to be delivered should be populated for the capacity requirements for 3rd year. The sizing of the server requirement for the 3rd year should be such that it meets 60% of the required tpm-c at the end of 5th year.
7		The BIDDER should provide requisite licenses for all the system software required for the database server including, but not limited to, Operating System, Clustering Software, etc.
	Additional	
1	Processor	Blades should be x-86/RISC/EPIC processor based servers with processor clock speed of at least 2.0 GHz or above..
2	Number of Processors	Offered Server should be configured with minimum 4 (Four) Processors. 8-core per processor
3	Memory	The servers should be equipped with minimum 32 GB DDR 3 RAM or higher RAM per core
4	Memory Scalability	Memory Should be Scalable up to 512 GB
5	PCI-Express Slots	Server Should Have Minimum 4 * PCI Express Slots
6		Each server should support partitioning. Each partition should be populated with minimum 8 number of Gigabit full-duplex Ethernet ports OR 2 x 10Gigabit ports for LAN connectivity. Each 10G port must be capable of carving out at least 4 logical NICs with configurable speeds from one physical port.
7		The server should have the capability to balance the load across multiple port interfaces in active-active mode and seamless failover without any data corruption or Database crashing.
8	FC-HBA Ports	Each Partition should be populated with redundant 8Gbps FC ports. The servers should have the capability to balance the load across multiple HBA interfaces in active-active mode and seamless failover without any data corruption or Application/Database crashing. Also they should have the capability to support storage arrays of all leading storage vendors including, but not limited to EMC, Hitachi, HP, IBM, Network Appliance, SUN,etc
9		BIDDER should ensure that Database servers are in active-active mode on two separate physical servers
10	Internal RAID	Internal RAID Controller should be able to do RAID 0, 1, 5 and 6
11	Internal / External HDD (For OS only)	Minimum 2 * 320 GB
12	Pre-Failure Warranty	Critical Components like CPU, Memory, SSD & PCI Slots should be covered under Pre-Failure Warranty

13	OS & Virtualization Infrastructure Support	Should be provided with latest version of 64-bit UNIX operating system supported by OEM. OEM supported Virtualization software should be supplied in solution. Both OS and Virtualization software should be supplied for full configured capacity of the system. Should be supporting open source heterogeneous environment.
14	I/O & Power Supply Redundancy	Server Should have redundant power supply and redundant I/O

#	Nature of Requirement	Minimum Requirements for SAN Array
1	Controllers	The proposed SAN array shall be configured with dual Active-Active controllers for redundancy with dedicated cache mirroring interface between controllers
2	Front-End & Back-End Ports	The proposed SAN array shall be configured with minimum 4x8 Gb/s FC front end host ports, & 8 x 8Gb/s FC Back end ports spread across dual controllers.
3	Cache & Cache backup	The proposed SAN array shall be configured with at least 32 GB total usable read / write cache for data, across dual controllers. Cache shall be mirrored between the controllers.
4	Offered Capacity	The proposed SAN array shall be configured with minimum 12 TB using 300 GB or more and 15k rpm dual ported FC/SAS drives.
		SAN storage with various combination of RAID configuration
5	Maximum Scalability	The storage system should be scalable up to minimum 300TB of RAW capacity using fiber channel/SAS disk drives.
6	Disk IOPS	The array should be configured to deliver at least 10000 disk IOPS at less than 10 milliseconds response.
		BIDDER should enclose OEM certification for the given performance for proposed configuration supported with published benchmark document.
7	RAID Levels	The Proposed SAN Array should support RAID Levels 1 or 10, 5 or 6
8	Snapshots & Volume Clones	Offered Storage must include snapshots & volume clones licenses

#	Nature of Requirement	Minimum Requirements for SAN Switch
1	Architecture	Switch Should have Completely Non-Blocking Architecture
2	Fabric Bandwidth	Switch Should have minimum 680 Gb/s Fabric Bandwidth
3	Port Speed	Ports should be configured with atleast 8 Gb/s FC SFPs and should auto-negotiate to 2/4 Gbps speeds
4	QoS	Switch Should support Quality of Services
5	ISL Trunking	Switch Should include ISL Trunking / link aggregation upto minimum 64Gb/s
6	Power Supply and Fans	Switch Should be Configured with redundant Power Supplies and Fans
7	Number of Ports	24 ports
8	Form Factor	Rack Mount

#	Nature of Requirement	Minimum Requirement Description for EMS
1	Basic Requirement	Solution should provide for future scalability of the whole system without major architectural changes.
2	Basic Requirement	Should be SNMP compliant.
3	Basic Requirement	Filtering of events should be possible, with advance sort option based on components, type of message, time etc.
4	Basic Requirement	Should support Web / Administration Interface.
5	Basic Requirement	Should provide compatibility to standard RDBMS.
6	Basic Requirement	Solution should be open, distributed, and scalable and open to third party integration.
7	Basic Requirement	Should provide fault and performance management for multi-vendor TCP/IP networks.
8	Security	Should be able to provide secured windows based consoles / secured web based consoles for accessibility to EMS.
9	Security	Should have web browser interface with user name and Password Authentication.
10	Security	Administrator/ Manager should have privilege to create/modify/delete user.
11	Polling Cycle	Support discriminated polling
12	Polling Cycle	Should be able to update device configuration changes such as re-indexing of ports
13	Fault Management	Should be able to get fault information in real time and present the same in alarm window with description, affected component, time stamp etc.
14	Fault Management	Should be able to get fault information from heterogeneous devices routers, switches, servers etc.
15	Fault Management	Event related to servers should go to a common enterprise event console where a set of automated tasks can be defined based on the policy.
16	Fault Management	Should have ability to correlate events across the entire infrastructure components of DC/DR.
17	Fault Management	Should support automatic event correlation in order to reduce events occurring in DC/DR.
18	Fault Management	Should support advanced filtering to eliminate extraneous data / alarms in Web browser and GUI.
19	Fault Management	Should be configurable to suppress events for key systems/devices that are down for routine maintenance or planned outage.
20	Fault Management	Should be able to monitor on user-defined thresholds for warning/ critical states and escalate events to event console of enterprise management system.
21	Fault Management	Should provide out of the box root cause analysis with multiple root cause algorithms inbuilt for root cause analysis.
22	Fault Management	Should have self-certification capabilities so that it can easily add support for new traps and automatically generate alarms.
23	Fault Management	Should provide sufficient reports pertaining to asset and change management, alarms and availability of critical network resources as well as network response times for critical links.
24	Fault Management	The tool shall integrate network, server and database performance information and alarms in a single console and provide a unified reporting interface for network and system components. The current performance state of the entire network and system infrastructure shall be visible in an integrated console.
25	Fault Management	Should provide an integrated performance view for all the managed systems and networks along with the various threshold violations alarms in them. It should be possible to drill-down into the performance view to execute context specific reports.

26	Fault Management	Should provide the following reports for troubleshooting, diagnosis, analysis and resolution purposes: Trend Reports, At-A-Glance Reports, & capacity prediction reports.
27	Fault Management	Should be able to auto-calculate resource utilization baselines for the entire managed systems and networks and allow user to set corresponding upper and lower threshold limits.
28	Discovery	Should provide accurate discovery of layer 3 and heterogeneous layer 2 switched networks for Ethernet, LAN, and Servers etc.
29	Discovery	Manual discovery can be done for identified network segment, single, or multiple devices.
30	Presentation	Should be able to discover links with proper colour status propagation for complete network visualization.
31	Presentation	Should support dynamic object collections and auto discovery. The topology of the entire Network should be available in a single map.
32	Presentation	Should give user option to create his /or her map based on certain group of devices or region.
33		
34	Agents	Should monitor various operating system parameters such as processors, memory, files, processes, file systems etc. where applicable using agents on the servers to be monitored.
35	Agents	Provide performance threshold configuration for all the agents to be done from a central GUI based console that provide a common look and feel across various platforms in the enterprise. These agents could then dynamically reconfigure them to use these threshold profiles they receive.
36	System Monitoring	Should be able to monitor/manage large heterogeneous systems environment continuously.
37	System Monitoring	Should monitor / manage following (based on Stack):
38	System Monitoring	Event log monitoring.
39	System Monitoring	Virtual and physical memory statistics
40	System Monitoring	Paging and swap statistics
41	System Monitoring	Operating system
42	System Monitoring	Memory
43	System Monitoring	Logical disk
44	System Monitoring	Physical disk
45	System Monitoring	Process
46	System Monitoring	Processor
47	System Monitoring	Paging file
48	System Monitoring	IP statistics
49	System Monitoring	ICMP statistics
50	System Monitoring	Network interface traffic
51	System Monitoring	Cache
52	System Monitoring	Active Directory / LDAP Services
53	System Monitoring	Should monitor following with statistics :
54	System Monitoring	CPU Utilization, CPU Load Averages
55	System Monitoring	System virtual memory (includes swapping and paging)
56	System Monitoring	Disk Usage
57	System Monitoring	No. of Nodes in each file system
58	System Monitoring	Network interface traffic
59	System Monitoring	Critical System log integration
60	Infrastructure Services	IIS / Tomcat / Apache / Web server statistics
61	Infrastructure Services	HTTP service
62	Infrastructure Services	HTTPS services & CRIMINAL TRACKING NETWORK AND SYSTEMS
63	Infrastructure Services	FTP server statistics
64	Infrastructure Services	POP/ SMTP Services
65	Infrastructure Services	ICMP services

66	Infrastructure Services	Database Services – Monitor various critical relational database management system (RDBMS) parameters such as database tables / table spaces, logs etc.
67	Application Performance Management	End to end Management of applications (J2EE/.NET based)
68	Application Performance Management	Determination of the root cause of performance issues whether inside the
69	Application Performance Management	Java / .Net application in connected back-end systems or at the network layer.
70	Application Performance Management	Automatic discovery and monitoring of the web application environment
71	Application Performance Management	Ability to monitor applications with a dashboard.
72	Application Performance Management	Ability to expose performance of individual SQL statements within problem transactions.
73	Application Performance Management	Monitoring of third-party applications without any source code change requirements.
74	Application Performance Management	Proactive monitoring of all end user transactions; detecting failed transactions; gathering evidence necessary for problem diagnose.
75	Application Performance Management	Storage of historical data is for problem diagnosis, trend analysis etc.
76	Application Performance Management	Monitoring of application performance based on transaction type.
77	Application Performance Management	Ability to identify the potential cause of memory leaks.
78	Reporting	Should able to generate reports on predefined / customized hours.
79	Reporting	Should be able to present the reports through web and also generate “pdf” / CSV / reports of the same.
80	Reporting	Should provide user flexibility to create his /or her custom reports on the basis of time duration, group of elements, custom elements etc.
81	Reporting	Should provide information regarding interface utilization and error statistics for physical and logical links.
82	Reporting	Should create historical performance and trend analysis for capacity planning.
83	Reporting	Should be capable to send the reports through e-mail to pre-defined user with pre-defined interval.
84	Reporting	Should have capability to exclude the planned-downtimes or downtime outside SLA.
85	Reporting	Should be able to generate web-based reports, historical data for the systems and network devices and Near Real Time reports on the local management console.
86	Reporting	Should be able to generate the reports for Server, Application.
87	Reporting	Provide Historical Data Analysis: The software should be able to provide a time snapshot of the required information as well as the period analysis of the same in order to help in projecting the demand for bandwidth in the future.
88	Availability Reports	Availability and Uptime – Daily, Weekly, Monthly and Yearly Basis
89	Availability Reports	Trend Report
90	Availability Reports	Custom report
91	Availability Reports	MTBF and MTTR reports
92	Performance Reports	Device Performance – CPU and Memory utilized
93	Performance Reports	Interface errors
94	Performance Reports	Server and Infrastructure service statistics
95	Performance Reports	Trend report based on Historical Information
96	Performance Reports	Custom report
97	Performance Reports	SLA Reporting
98	Performance Reports	Computation of SLA for entire DC/DR Infrastructure

99	Performance Reports	Automated Daily, Weekly, Monthly, Quarterly and Yearly SLA reports.
100	Data Collection	For reporting, required RDBMS to be provided with all licenses.
101	Data Collection	Should have sufficient Storage capacity should to support all reporting data
102	Integration	Should be able to receive and process SNMP traps from infrastructure components such as router, switch, servers etc.
103	Integration	Should be able integrate with Helpdesk system for incidents.
104	Integration	Should be able to send e-mail or Mobile –SMS to pre-defined users for predefined faults.
105	Integration	Should trigger automated actions based on incoming events / traps. These actions can be automated scripts/batch files.
106	Network Management	The Network Management function must monitor performance across heterogeneous networks from one end of the enterprise to the other.
107	Network Management	It should proactively analyze problems to improve network performance.
108	Network Management	The Network Management function should create a graphical display of all discovered resources.
109	Network Management	The Network Management function should have extensive reporting facility, providing the ability to format and present data in a graphical and tabular display.
110	Network Management	The Network Management function should collect and analyze the data. Once collected, it should automatically store data gathered by the NMS system in a database. This enterprise-wide data should be easily accessed from a central location and used to help with capacity planning, reporting, and analysis.
111	Network Management	The Network Management function should also provide information on performance of Ethernet segments, including capacity utilization and error statistics for the segment, WAN links and routers.
112	Network Management	Alerts should be shown on the Event Management map when thresholds are exceeded and should subsequently be able to inform Network Operations Center (NOC) and notify concerned authority using different methods such as emails, etc.
113	Network Management	It should be able to automatically generate a notification in the event of a link failure to ensure proper handling of link related issues.
114	Network Management	The Systems and Distributed Monitoring (Operating Systems) of EMS should be able to monitor:
115	Network Management	Processors: Each processor in the system should be monitored for CPU utilization. Current utilization should be compared against user-specified warning and critical thresholds.
116	Network Management	File Systems: Each file system should be monitored for the amount of file system space used, which is compared to user-defined warning and critical thresholds.
117	Network Management	Log Files: Logs should be monitored to detect faults in the operating system, the communication subsystem and in applications. The function should also analyze the files residing on the host for specified string patterns.
118	Network Management	System Processes: The System Management function should provide real-time collection of data from all system processes. This should identify whether or not an important process has stopped unexpectedly. Critical processes should be automatically restarted using the System Management function.
119	Network Management	Memory: The System Management function should monitor memory utilization and available swap space.

120	SLA Monitoring	The SLA Monitoring component of EMS will have to possess the following capabilities:
121	SLA Monitoring	EMS should integrate with the application software component of portal software that measures performance of system against the following SLA parameters:
122	SLA Monitoring	Response times of Portal;
123	SLA Monitoring	Uptime of IT Infrastructure;
124	SLA Monitoring	Meantime for restoration of services etc.
125	SLA Monitoring	EMS should compile the performance statistics from all the IT systems involved and compute the average of the parameters over a quarter, and compare it with the SLA metrics laid down in the RFP.
126	SLA Monitoring	The EMS should compute the weighted average score of the SLA metrics and arrive at the quarterly service charges payable to the Agency after applying the system of penalties and rewards.
127	SLA Monitoring	The SLA monitoring component of the EMS should be under the control of the authority that is nominated the client so as to ensure that it is in a trusted environment.
128	SLA Monitoring	The SLA monitoring component of the EMS should be subject to random third party audit to vouchsafe its accuracy, reliability, and integrity.
129	ITIL based Helpdesk	Helpdesk system would automatically generate the incident tickets and log the call. Such calls are forwarded to the desired system support personnel deputed by the Implementation Agency. These personnel would look into the problem, diagnose and isolate such faults and resolve the issues timely. The helpdesk system would be having necessary workflow for transparent, smoother and cordial DC/DR support framework.
130	ITIL based Helpdesk	The Helpdesk system should provide flexibility of logging incident manually via windows GUI and web interface.
131	ITIL based Helpdesk	The web interface console of the incident tracking system would allow viewing, updating, and closing of incident tickets.
132	ITIL based Helpdesk	The trouble-ticket should be generated for each complaint and given to asset owner immediately as well as part of email.
133	ITIL based Helpdesk	Helpdesk system should allow detailed multiple levels/tiers of categorization on the type of security incident being logged.
134	ITIL based Helpdesk	It should provide classification to differentiate the criticality of the security incident via the priority levels, severity levels and impact levels.
135	ITIL based Helpdesk	It should allow SLA to be associated with a ticket based on priority, severity, incident type, requestor, asset, location or group individually as well as collectively.
136	ITIL based Helpdesk	It should maintain the SLA for each item/service. The system should be able to generate report on the SLA violation or regular SLA compliance levels.
137	ITIL based Helpdesk	It should be possible to sort requests based on how close are the requests to violate their defined SLA’s.
138	ITIL based Helpdesk	It should support multiple time zones and work shifts for SLA & automatic ticket assignment.
139	ITIL based Helpdesk	It should allow the helpdesk administrator to define escalation policy, with multiple levels & notification, through easy to use window GUI / console.
140	ITIL based Helpdesk	System should provide a knowledge base to store history of useful incident resolution.
141	ITIL based Helpdesk	It should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
142	ITIL based Helpdesk	The web-based knowledge tool would allow users to access his / her knowledge article for quick references.

143	ITIL based Helpdesk	It should provide functionality to add / remove a knowledge base solution based on prior approval from the concerned authorities.
144	ITIL based Helpdesk	Provide seamless integration to generate events/incident automatically from NMS / EMS.
145	ITIL based Helpdesk	Each incident could be able to associate multiple activity logs entries manually or automatically events / incidents from other security tools or EMS / NMS.
146	ITIL based Helpdesk	Allow categorization on the type of incident being logged.
147	ITIL based Helpdesk	Provide audit logs and reports to track the updating of each incident ticket.
148	ITIL based Helpdesk	Proposed incident tracking system would be ITIL compliant.
149	ITIL based Helpdesk	It should be possible to do any customizations or policy updates in flash with zero or very minimal coding or down time.
150	ITIL based Helpdesk	It should integrate with Enterprise Management System event management and support automatic problem registration, based on predefined policies.
151	ITIL based Helpdesk	It should be able to log and escalate user interactions and requests.
152	ITIL based Helpdesk	It should support tracking of SLA (service level agreements) for call requests within the help desk through service types.
153	ITIL based Helpdesk	It should be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.
154	ITIL based Helpdesk	It should provide status of registered calls to end-users over email and through web.
155	ITIL based Helpdesk	The solution should provide web based administration so that the same can be performed from anywhere.
156	ITIL based Helpdesk	It should have a customized Management Dashboard for senior executives with live reports from helpdesk database.
157		
158	Client Management System	The proposed desktop management system should provide single integrated agent for asset management, remote software deployment and remote desktop control.
159		:
160	Asset Management System	The proposed Asset Management solution must provide inventory of hardware and software applications on end-user desktops including information on processor, memory, operating system, mouse, key board of desktops etc. through agents installed on them.
161	Asset Management System	The proposed Asset Management solution must have reporting capabilities; provide predefined reports and the possibility to create customized reports on data in the inventory database. Report results could be displayed as lists or graphs.
162	Asset Management System	The proposed Asset Management solution must have the capability to export the reports to CSV, HTML and XML format.
163	Asset Management System	The proposed Asset Management solution must provide the facility for user defined templates to collect custom information from desktops.
164	Asset Management System	The proposed Asset Management solution must provide facility to recognize custom applications on desktops.
165	Asset Management System	The proposed Asset Management solution must support administrators to register a new application to the detectable application list using certain identification criteria’s (Like executable, Date/time stamp etc.). The new application must be detected automatically from next time the inventory is scanned.

166	Asset Management System	The proposed Asset Management solution must provide facility for queries and automated policies to be set up and permit scheduling of collecting engines to pick up the data at defined intervals.
167	Asset Management System	The proposed Asset Management solution must be able to collect WBEM information.
168	Asset Management System	The proposed Asset Management solution must integrate with the helpdesk solution and allow ticket creation automatically on an event defined in asset management solution. It should also allow manual ticket creation also.
169	Asset Management System	The proposed Asset Management solution must support Software metering to audit and control software usage where launching of an application can be prevented based on centrally configured number of licenses for an application.
170	Remote Software Deployment System	It should provide delivery, installation, and un-installation of software (ex. Patches of Anti-virus solution etc.) installed on end-user desktops by software delivery remotely through agents installed on them. It must allow pre- and post-installation steps to be specified if required & support rollback in the event of failure in installing software to end-user desktops.
171	Remote Software Deployment System	The tool should have the capability to install applications based on interdependencies i.e. to be installed in a particular order.
172	Remote Software Deployment System	It should support deployment of MSI based packages using drag and drop method.
173	Remote Software Deployment System	It should perform actual distribution of software remotely, not mere file transfer and manual installation at other end. Automated installation should be possible.
174	Remote Software Deployment System	It should include a Software packager for creating software packages to be delivered to end-user desktops which uses a snap-shot technology.
175	Remote Software Deployment System	It should support both push and pull software distribution modes. A catalog/advertisement option of the existing software delivery packages must be provided for end-user to download and install software of his / her choice.
176	Remote Software Deployment System	Users must be allowed to cancel jobs if they are launched at an inconvenient time. Cancelled jobs must be allowed to be reactivated. Forcing packages onto the computer must also be possible.
177	Remote Desktop Control Management System	The proposed solution should allow remote control of end-user desktop for facilitating resolution of desktop issues without the need to go to the end-user desktop, through agents installed on them.
178	Remote Desktop Control Management System	It should provide the capability of taking Remote control of Linux systems also using Views sitting on Windows platform.
179	Remote Desktop Control Management System	It should provide Windows integrated authentication as well as application based authentication option to choose from for the agent installed.
180	Remote Desktop Control Management System	It should allow host enabled recording which allows the end user to initiate a recording session.
181	Remote Desktop Control Management System	It should have the ability to convert the recorded sessions in AVI/WMA format so it can be replayed using commonly available Windows media player.
182	Remote Desktop Control Management System	Centralized User Management should allow administrators to centrally manage remote control users’ and their access rights. Administrators must be able to define preferences and capabilities different users or user groups have, as well as defining which targets they can control.

183	Remote Desktop Control Management System	It should support Seamless integration with management applications such as helpdesk, asset management and Software delivery.
184	Remote Desktop Control Management System	It should support remote Reboot & Chat functions between nodes.
185	Remote Desktop Control Management System	It should provide facility for encrypting the authentication traffic and support AES 256.

#	Nature of Requirement	Minimum Requirement Description for Backup Solution
1	Support of SAN Based Backup	Proposed backup solution should provide Online SAN based backup agent on all database servers with LAN based (open file support) on all
2	Linux Compatible Software	The proposed Backup Solution Software has inbuilt Java / Web based GUI for centralized management of backup domain and Linux
3	Disk Staging Feature	Software must have integrated true Disk Staging feature, wherein the backup continues to take place even when the disk space allocated is full. The backup software must be intelligent enough to flush out the data from the disk and migrate the same to the tape automatically based on the user defined threshold & will not affect the backup operations. Bidder must quote the licenses for disk based backup
4	Disk Staging Feature	The proposed Backup Solution has in-built media management and supports cross platform Device & Media sharing in SAN environment. It provides a centralized scratched pool thus ensuring backups never fail
5	Incremental Backup	The software should support for ever incremental backup & there should not be a need to do a Full backup again
6	Entire Server Backup	The software should have capability to backup the entire configuration of the server and restore it from scratch the entire system including configuration when in a scenario of hardware failure
7	Entire Server Backup	Backup Software is able to rebuild the Backup Database/Catalog from tapes in the event of catalog loss/corruption.
8	Database support	The proposed Backup Solution has certified “Hot-Online” backup solution for different type of Databases such as Oracle, MySQL,
9	Database support	The proposed solution should have Bare Metal Recovery agent on database servers
10	Individual File Restore	The Proposed backup solution shall provide granularity of single file
11	Individual File Restore	The Proposed backup solution shall be designed in such a fashion so that every client/server in a SAN can share the robotic
12	Individual File Restore	Backup Solution shall be able to copy data across firewall
13	Individual File Restore	Backup Solution shall support automatic skipping of backup during
14	Individual File Restore	Should support backup Polices to be defined centrally & should be applied to Data, not restricted to tape media’s. This is to optimally
15	Individual File Restore	The software should have capability to retrieve selectively based on search criteria
16	Individual File Restore	The Backup Software shall provide restart-able restore in case of any failure during a Restore operation
17	Individual File Restore	The Backup software must also be capable of reorganizing the data onto tapes within the library by migrating data from one set of tapes into another, so that the space available is utilized to the maximum. The software must be capable of setting this utilization threshold for
18	Individual File Restore	The backup software should have the capability to reclaim the media back in to the new backup process even if the 50% of the data had expired in the backed up media. The reclamation threshold should be
19	Individual File Restore	The Backup software must have an integrated RDBMS as the catalog and must not use Flat file system to store the backup data.
20	Individual File Restore	Should have the ability to retroactively update changes to data management policies that will then be applied to the data that is already being backed up or archived

#	Nature of Requirement	Minimum Requirement Description for Multi-function Printer
1	Printer Specifications	
	Print speed, black	18 ppm or more
	Print resolution, black	Up to 600 x 600 dpi
	Print technology	Laser
	Monthly duty cycle	8000 pages or more
	Memory, standard	32 MB or more
	Print languages, standard	Host-based printing, PCL 5e
	Duplex printing (printing on both sides of paper)	Manual (driver support)
	Media sizes, standard	A4, Letter
	Media sizes, custom	250-sheet input tray: 5.8 x 8.27 to 8.5 x 14 in; priority feed slot: 3 x 5 to 8.5 x 14 in
2	Scanner Specifications	
	Scanner type	Flatbed, ADF
	Scan resolution, optical	1200 dpi or more
	Scan size	8.5 x 11.7 in
	Scan speed	6ppm or above
	Supported file formats	PDF; TIF; BMP; GIF; JPG
3	Copier Specifications	
	Copy resolution	600x 400 dpi or more
4	Other Specifications	
	Network ready	Standard (built-in Ethernet)
	ENERGY STAR® Qualified	Yes
	Warranty Coverage	Comprehensive warranty for 3 years.

#	Nature of Requirement	Minimum Requirement Description for Intranet Firewall
1	General Requirements	The firewall should integrate with multiple full-featured, high-performance security services, including application-aware firewall, SSL and IPsec VPN
2	General Requirements	The FW should support a comprehensive command line interface (CLI), verbose syslog, and Simple Network Management Protocol (SNMP).
3	General Requirements	The FW should be a 2 slot chassis in 1/2 RU, 19-in. rack-mountable form factor
4	General Requirements	Should have a minimum real world Multi- protocol throughput of 10 Gbps. Real world profile should include but not limited to HTTP, Bit Torrent, FTP , SMTP and IMAPv4. Throughout should be further scabale to double with clustering whenever required in future.
5	General Requirements	Maximum 3DES/AES throughput of 2gbps
6	General Requirements	Maximum interfaces 10-port 10/100/1000 and 8-port 10 Gigabit Ethernet SFP+ and should be future scalable to 20 SFP+ ports.
7	General Requirements	Maximum vlans 1000
8	General Requirements	Maximum concurrent sessions 3,000,000
9	General Requirements	Should have 10 Virtual Firewalls Day1 scalable to 150
10	General Requirements	The software on the firewall should support online software reconfiguration to ensure that changes made to a firewall configuration take place with immediate effect.
11	General Requirements	Should support Active/Active and Active/Standby Failover
12	General Requirements	Firewall and VPN Active/Standby failover services should be supported without any additional licenses
13	General Requirements	Should have redundant power supply
14	General Requirements	Should have 2 USB 2.0 ports or better
15	General Requirements	The device should have a dedicated console port
16	General Requirements	Should support integrated Ipsec and Client and Clientless SSL VPN
17	General Requirements	Should support minimum 7,000 vpn tunnels
18	General Requirements	Botnet Filtering capabilities are must. It should have it's own reputation/ dynamic database to provide dynamic filter database about Botnets providing protection against spyware, adware, malware, data tracking, adult content that are used for distribution of above etc
19	General Requirements	Should support checking of incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses, and then logs any suspicious activity.
20	General Requirements	Should support Routed and Transparent mode
21	General Requirements	Firewall should support Web based (HTTP and HTTPS) configuration, and management
22	General Requirements	Firewall should support Command Line Interface using console, Telnet and SSH
23	General Requirements	Should be managed using a centralized management system
24	General Requirements	Should support Syslog server logging
25	General Requirements	The Firewall should support site-to-site vpn as well as Remote access vpn on the same appliance
26	General Requirements	There Performance should not be significantly affected by enabling the firewall features, SSL and IPsec encryption should be performed by dedicated hardware processors. IPS should performed by dedicated add-in modules, each with its own processors, storage, and memory
27	General Requirements	The firewall should have support for cut-through proxy and user authentication
28	General Requirements	Should support dynamic downloading and enforcement of ACLs on a per-user basis once the user is authenticated with the appliance.
29	VPN Features	Should support minimum 7000 VPN tunnels
30	VPN Features	The device should support IPSEC/IKEv2 for remote VPN access
31	VPN Features	The security appliance supports the following encryption standards for ESP: DES, 3DES, AES-128, AES-192, AES-256

32	VPN Features	The security appliance supports the following hashing algorithms: MD5, SHA
33	VPN Features	Supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates.
34	VPN Features	Firewall should support Suite B cryptography including ECDSA, ECDH & SHA- 2
35	VPN Features	Firewall Should support IPSecv3 and enhanced IPSecv3 features, which are defined as ESPv3
36	Support	The system should not be an end of life / end of service product.

#	Nature of Requirement	Minimum Requirement Description for Internet Firewall
1	Internet Firewall	The firewall should integrate with multiple full-featured, high-performance security services, including application-aware firewall, SSL and IPsec VPN
2	Internet Firewall	The FW should support a comprehensive command line interface (CLI), verbose syslog, and Simple Network Management Protocol (SNMP).
3	Internet Firewall	The FW should be a 2 slot chassis in 1/2 RU, 19-in. rack-mountable form factor
4	Internet Firewall	Should have a maximum throughput of 4gbps and Multi- protocol throughput of 2gbps. Real world profile should include but not limited to HTTP, Bit Torrent, FTP , SMTP and IMAPv4
5	Internet Firewall	Maximum 3DES/AES throughput of 600 Mbps
6	Internet Firewall	Maximum concurrent sessions 1,000,000
7	Internet Firewall	New connections per second 45,000
8	Internet Firewall	Packets/sec (64byte) 1,500,000
9	Internet Firewall	Minimum interfaces 6-port 10/100/1000, scalable to additional 6 x 1 GiagEthernet ports with option of SFP as well
10	Internet Firewall	Maximum vlans 500
11	Internet Firewall	Should have 2 Virtual Firewalls Day1 scalable to 100
12	Internet Firewall	The software on the firewall should support online software reconfiguration to ensure that changes made to a firewall configuration take place with immediate effect.
13	Internet Firewall	Should support Active/Active and Active/Standby Failover
14	Internet Firewall	Firewall and VPN Active/Standby failover services should be supported without any additional licenses
15	Internet Firewall	Should have 2 USB 2.0 ports
16	Internet Firewall	The device should have a dedicated console port
17	Internet Firewall	Should support integrated Ipsec and Client and Clientless SSL VPN
18	Internet Firewall	Should support minimum 3,000 cumulative vpn including IPSEc and SSL and licensed for 500 SSL VPN from Day1
19	Internet Firewall	Should be able to block popular peer-to-peer applications and should have botnet filter capabilities. Botnet Filtering capabilities should also include blocking communication between the infected Bots and the Command & Control Center.
20	Internet Firewall	The Firewall should be able to filter traffic even if the packets are fragmented.
21	Internet Firewall	Should support checking of incoming and outgoing connections against a dynamic database of known bad domain names and IP addresses, and then logs any suspicious activity.
22	Internet Firewall	Should support Routed and Transparent mode
23	Internet Firewall	Firewall should support Web based (HTTP and HTTPS) configuration, and management
24	Internet Firewall	Firewall should support Command Line Interface using console, Telnet and SSH
25	Internet Firewall	Should be managed using a centralized management system
26	Internet Firewall	Should support Syslog server logging
27	Internet Firewall	The FW should support site-to-site vpn as well as Remote access vpn on the same appliance
28	Internet Firewall	There Performance should not be significantly affected by enabling the firewall features, SSL and IPsec encryption should be performed by dedicated hardware processors. IPS should performed by dedicated add-in modules, each with its own processors, storage, and memory
29	Internet Firewall	Should support dynamic downloading and enforcement of ACLs on a per-user basis once the user is authenticated with the appliance.
30	Internet Firewall	Should support minimum 3,000 Comulative vpn including IPSEc and SSL and licensed for 500 SSL VPN from Day1
31	Internet Firewall	The device should support IPSEC/IKEv2 for remote VPN access
32	Internet Firewall	Firewall Should support IPSecv3 and enhanced IPSecv3
33	Internet Firewall	The security appliance supports the following encryption standards for ESP: DES, 3DES, AES-128, AES-192, AES-256 or better

34	Internet Firewall	The security appliance supports the following hashing algorithms: MD5, SHA
35	Internet Firewall	Supports the use of SHA-2 compliant signature algorithms to authenticate SSL VPN connections that use digital certificates.
36	Internet Firewall	The Firewall should also support the standard Layer 3 mode of configuration with Interface IP’s. It should be possible to protect the firewall policies from being compromised.

#	Nature of Requirement	Minimum Requirement Description for Intrusion Prevention System
1	Hardware features	IPS solution can be proposed as dedicated appliance/ as software license in Firewall or as additional Module in Intranet firewall. Following are the required features for IPS:
2	Advanced Threat Protection	IPS detection rules must be based on an extensible, open language that enables users to create their own rules, as well as to customize any vendor-provided rules.
3	Advanced Threat Protection	Detection rules provided by the vendor must be documented, with full descriptions of the identity, nature, and severity of the associated vulnerabilities and threats being protected against.
4	Advanced Threat Protection	The detection engine must be capable of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).
5	Advanced Threat Protection	The detection engine must incorporate multiple approaches for detecting threats, including at a minimum exploit-based signatures, vulnerability-based rules, protocol anomaly detection, and behavioral anomaly detection techniques. Identify and explain each type of detection mechanism supported.
6	Advanced Threat Protection	The detection engine must be resistant to various HTML-based attacks.
7	Advanced Threat Protection	The solution must be capable of detecting and blocking IPv6 attacks.
8	Advanced Threat Protection	The solution must provide IP reputation feed that comprised of several regularly updated collections of IP addresses determined by the proposed security vendor to have a poor reputation.
9	Advanced Threat Protection	The solution must support IP reputation intelligence feeds from third party and custom lists of IP addresses including a global blacklist.
10	Advanced Threat Protection	The solution must be capable of providing network-based detection of malware by checking the disposition of known files in the cloud using the SHA-256 file-hash as they transit the network
11	Intelligent Security Automation	The solution must be capable of employing an extensive set of contextual information (e.g., pertaining to the composition, configuration, and behavior of the network and its hosts) to improve the efficiency and accuracy of both manual and automatic analysis of detected events.
12	Intelligent Security Automation	The solution must be capable of significantly reducing operator effort and accelerating response to threats by automatically prioritizing alerts, ideally based on the potential for correlated threats to successfully impact the specific hosts they are directed toward.
13	Intelligent Security Automation	The solution must be capable of dynamically tuning IDS/IPS sensors (e.g., selecting rules, configuring policies, updating policies, etc.) with minimal human intervention.
14	Intelligent Security Automation	The solution must be capable of automatically providing the appropriate inspections and protections for traffic sent over non-standard communications ports.
15	Control Compliance	The solution must support creation of user-defined application protocol detectors.
16	Control Compliance	The solution must have content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.
17	Control Compliance	Protocols: HTTP, SMTP, IMAP, POP
18	Control Compliance	Direction: Upload, Download, Both
19	Control Compliance	File Types: Office Documents, Archive, Multimedia, Executable, PDF, Encoded, Graphics, video and System Files.
20	Control Compliance	The proposed solution should provide an option to include URL filtering for enforcing Internet content filtering so as to reduce web born threats and improve productivity.
21	Control Compliance	Each URL in the data set must has an associated category and reputation. URL category is a general classification for the URL while URL reputation represents how likely the URL is to be used for purposes that might be against the organization’s security policy.
22	Control Compliance	The solution must provide capabilities for establishing and enforcing host compliance policies and alerting on violations.

23	Control Compliance	The solution must be capable of exempting specific hosts from specific compliance rules and suppressing corresponding compliance events and alerts.
24	Control Compliance	The solution must be capable of easily identifying all hosts that exhibit a specific attribute or non-compliance condition.
25	Management and Usability	The management platform must be capable of centralized, life cycle management for all sensors.
26	Management and Usability	The management platform must be delivered in virtual appliance form factor (management system and UI must provide the same features and functions as in the physical appliance).
27	Management and Usability	The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events.
28	Management and Usability	The management platform must be accessible via a web-based interface and ideally with no need for additional client software.
29	Management and Usability	The management platform must provide a highly customizable dashboard.
30	Management and Usability	The management platform must be capable of integrating third party vulnerability information into threat policy adjustment routines and automated tuning workflows.
31	Reporting and Alerting	The management platform must provide robust reporting capabilities, including a selection of pre-defined reports and the ability for complete customization and generation of new reports.
32	Reporting and Alerting	The management platform must allow quick report customization by importing from dashboards, workflows and statistics summaries.
33	Reporting and Alerting	The management platform must provide multiple report output types or formats, such as PDF, HTML, and CSV.
34	Reporting and Alerting	The management platform must support multiple mechanisms for issuing alerts (e.g., SNMP, e-mail, SYSLOG).
35	Reliability and Availability	Sensors must support built-in capability of failing open, such that communications traffic is still allowed to pass if the inline sensor goes down.
36	Reliability and Availability	The product must support “Lights Out Management” capability where remote upgrade, restore, and downgrade functionality without physical access to the appliance being required.
37	Reliability and Availability	The management platform must be capable of monitoring the health of all components and issuing alerts for anomalous conditions.
38	Reliability and Availability	Intra-system communications must be secure.
39	Reliability and Availability	The supplier must have a detailed process for customer submission of product-related faults and the resolution of those faults, including provisions for escalation of critical or unresolved issues.
40	Performance	Should have minimum Inspected throughput of 2 Gbps for all kinds of real word traffic.
41	Performance	Should support minimum 1,000,000 Concurrent Connections.
42	Performance	Should have minimum 6 monitoring interface of 1 Gbps and should be modular platfrom to support scalability of additional 1 G & 10G interfaces
43	Performance	Should support minimum 45,000 new Connections/Sec.
44	Performance	Must have dedicated 10/100/1000 RJ45 Management Interface.
45	Performance	Should support Dual power supplies for redundancy

#	Nature of Requirement	Minimum Requirement Description for Optical Fibre Cable
1	Cable Type	Optical Fiber Single Mode 24 Core
2	Core	24
3	Mode	Single Mode
4	Cladding diameter	125.0 µm ± 1.0
5	Coated fibre diameter	245 µm ±10
6	Core/cladding concentricity error	≤ 0.8µm
7	Coating/cladding concentricity error	≤ 12µm
8	Cladding non-circularity	≤ 1.0 %
9	Mode Field Diameter	9.3µm ± 0.5 at 1310nm
10	Attenuation (cable)	0.36dB/Km at 1310nm, 0.25dB/Km at 1550nm,
11	Zero-Dispersion Wavelength	1300 to 1322 nm
12	Zero-Dispersion Slope	≤0.092 ps/Sq. Nm .km
13	Zero-Dispersion Slope	≤0.092 ps/Sq. Nm .km
14	Cut-off Wavelength	≤1260 nm
15	Polarization Mode Dispersion Coefficient	≤0.2 at 1310nm
16	Fibre macro bend loss	≤0.05dB at 1550 nm with 75 mm dia, 100 turns
17	Fibre macro bend loss	≤0.5dB at 1550 nm with 32 mm dia, 1 turn

#	Nature of Requirement	Minimum Requirement Description for Intranet Router
1	Functional Requirements	The router shall support 1:1 route processor/control processor redundancy, 1:1/1:N switch fabric and PSU redundancy and 1:1 service module redundancy in case any services asked for in the RFP is delivered through a service module
2	Functional Requirements	The Core router must be based on architecture which does hardware based forwarding and switching. The processing engine architecture must be multi processor based for enhanced performance.
3	Functional Requirements	The Core router must have onboard support for intelligent traffic measurement and analysis. The router must support flow based traffic analysis feature.
4	Functional Requirements	The router must have hardware assisted Network Address Translation (NAT) capability as per RFC 1631.
5	Hardware Architecture	Backplane Architecture: The back plane architecture of the router must be modular and redundant. The back plane bandwidth must be 20Gbps from day 1 and scalable to 40 Gbps
6	Hardware Architecture	Number of Slots: The router must be chassis based with minimum 4 numbers of slots.
7	Hardware Architecture	The router must have redundant power supply module. The router must support 220V AC or -48V DC power supply module. There should not be any impact on the router performance in case of one power supply fails.
8	Hardware Architecture	The router processor architecture must be multi processor/ multi core based and should support hardware accelerated, parallelized and programmable IP forwarding and switching.
9	Hardware Architecture	The router in the event of failure of any one processor should switchover to the redundant processor without dropping any traffic flow. There should not be any impact on the performance in the event of active routing engine.
10	Hardware Architecture	The router must support on line hot insertion and removal of cards. Any insertion line card should not call for router rebooting nor should disrupt the remaining unicast and multicast traffic flowing in any way.
11	Hardware Architecture	The router must have support for flash memory for configuration and OS backup.
12	Router Performance	Should support up to 18 Mpps of Forwarding performance
13	Router Performance	The Router solution must be a carrier-grade Equipment supporting the following: Hitless interface protection, In-band and out-band management, Software rollback feature, Graceful Restart for OSPF, BGP, LDP, MP-BGP etc.
14	Router Performance	The router should support uninterrupted forwarding operation for OSPF, IS-IS routing protocol to ensure high-availability during primary controller card failure.
15	Physical Interface Support	The router line card must support following interface as defined in the IEEE, ITU-T: Fast Ethernet - 10BaseT/100BaseT Ethernet as defined in IEEE 802.3 , Gigabit Ethernet - 1000BaseSX, 1000BaseLX, 1000BaseZX as defined in IEEE 802.3
16	Physical Interface Support	The router should support Channelized STM1 interfaces to aggregate multiple E1 / sub-rate E1 circuits coming in from remote locations.
17	Physical Interface Support	Support for 10 Gigabit Ethernet interface.
18	Layer 3 Routing Protocols	The router must support the IPv4 and IPv6 stack in hardware and software. It must support both IPv4 and IPv6 routing domains separately and concurrently. It must also support the ability to bridge between IPv4 and IPv6 routing domains.
19	Layer 3 Routing Protocols	The router must support RIPv1 & RIPv2, OSPF, BGPv4 and IS-IS routing protocol.
20	IPv6 Support	Should support IP version 6 in hardware.
21	IPv6 Support	Should support IPv6 static route, OSPFv3, IS-IS support for IPv6, Multiprotocol BGP extensions for IPv6, IPv6 route redistribution.

22	IPv6 Support	The router shall support dual stack IPv6 on all interfaces and IPv6 over IPv4 tunneling, IPv6 Multicast protocols – Ipv6 MLD, PIM-Sparse Mode, and PIM – SSM,Pv6 Security Functions – ACL, IPv6 Firewall, SSH over IPv6, MPLS Support for IPv6 - IPv6 VPN over MPLS, Inter-AS options, IPv6 VPN over MPLS, IPv6 transport over MPLS
23	IPv6 Support	The router should support for IPv6 Multicast.
24	IPv6 Support	Should support IPv6 Quality of Service
25	IPv6 Support	Should perform IPv6 transport over IPv4 network (6 to4 tunneling).
26	IPv6 Support	Should support SNMP over IPv6 for management.
27	Quality of Service	The router must be capable of doing Layer 3 classification and setting ToS/Diffserve bits on incoming traffic using configured guaranteed rates and traffic characteristics. The marking of the ToS/Diffserve bits should be non-performance impacting.
28	Quality of Service	The scheduling mechanism must allow for expedited or strict priority routing for all high priority traffic.
29	Quality of Service	The scheduling mechanism must allow for alternate priority routing traffic necessary to keep from starving other priority queues.
30	Quality of Service	The router must provide facility to prioritize the SNMP traffic.
31	Multicast Support	The multicast implementation must support source specific multicast.
32	Multicast Support	The router must support IGMPv2 and IGMPv3.
33	MPLS Feature	Should support all standard protocols
34	Security Feature	Should support Access Control Lists at layer 2-4 in hardware. The access list parameters may be any combination of source and destination IP or subnet, protocol type (TCP/UDP/IP etc), source and destination port. There should not be any impact on the router performance upon enabling Access Lists.
35	Security Feature	The router should support multiple levels of access or role based access mechanisms.
36	Security Feature	Should support CPU Rate limiting and control plane policing feature to make sure the router is always available for management.
37	Security Feature	The proposed router should support for NAT from day one, Version of software for supplied router should be latest release to support all required features
38	Security Feature	The proposed router should have embedded support for 4000 IPsec tunnels from day one, Version of software for supplied router should be latest release to support all required features
39	Router Management Feature	Console Port: It should be possible to manage a particular system locally through console port or through a telnet session over LAN/WAN.
40	Router Management Feature	The router must support management through SNMPv1, v2 and v3
41	Router Management Feature	The router must support RADIUS and TACACS. The router must role based access to the system for configuration and monitoring.
42	Router Management Feature	The router must support Network Time Protocol (NTP) as per RFC 1305.
43	Router Management Feature	The router must have DHCP server functionality so that it can be used to lease IP addresses to the end points of local area network whenever required.
44	Port requirment from Day 1	Each Core router should be provided with 8 x 1G ports and 2 x 10G ports from Day 1
45	Industry Standards & Certifications	The Router should be minimum EAL3 / Applicable Protection Profile certified under the Common Criteria Evaluation Program
46	Support	The system should not be an end of life / end of service product.

#	Nature of Requirement	Minimum Requirement Description for Internet Router
1	Hardware features	Router should support hardware encryption acceleration for Ipsec & SSL VPNs internally or externally if an external VPN appliance is proposed the same should be an ASIC based appliance with the support of 500 minimum SSL VPNs tunnel
2	Hardware features	Router should support hardware encryption acceleration for Ipsec & SSL VPNs internally or externally if an external VPN appliance is proposed the same should be an ASIC based appliance
3	Hardware features	Router should support atleast Four 10/100/1000 Routed ports on-board out of which two should be available to be used as SFP ports.
4	Hardware features	Router should support default memory of 1GB Ram & scalable up to 2Gb Ram
5	Hardware features	Router should have atleast 4 slots for additional modules and one module should be loaded with 8 port 10/100/1000 Mbps LAN ports
6	Hardware features	Router should have support for WAN Interfaces
7	Hardware features	Router should support minimum performance of 1.8Mpps
8	Hardware features	Router should support internal redundant power supply.
9	Routing Protocols	Router should support following routing protocols & features:RIP, OSPF, BGP,ISIS, Policy based routing
10	IPv6 Routing Features	Router should support following IPv6 Features:OSPFv3, IPv6 support for ISIS, IPv6 support for BGP, IPv6 policy based routing, IPv6 Dual Stack
11	Multicast Features	Should support multicast BGP, Multicast NAT, PIM, IGMPv3
12	VPNS & Tunneling Features	Should support standard VPN Protocols & Features Ipsec Vpn, should support ipv6 for Ipsec
13	Qos Features	Should support the functionality of recognizing network based applications passing through router & provide statictics of traffic usage
14	Network Management Features	Router should support the ability to monitor events and take informational, corrective action when the monitored events occur or when a threshold is reached.
15	Network Management Features	Should support Netflowv9 or equivalent to provide data to enable network and security monitoring, network planning, traffic analysis, and IP accounting.
16	Network Management Features	Should support SNMPv3, SNMP over IPV6.
17	Network Management Features	Should support the functionality of measuring service level indicators including delay, jitter & availability
18	Network Management Features	Should support functionality to monitor network performance for VOIP, Video & VPN Network monitoring
19	Industry Standards & Certifications	The Router should be minimum EAL3 / Applicable Protection Profile certified under the Common Criteria Evaluation Program

#	Nature of Requirement	Minimum Requirement Description for Core Switch
1	Hardware features	Proposed network device must be 19'' rack mountable
2	Hardware features	Network Infrastructure equipment must use 240V AC power.
3	Hardware features	Must have Redundancy Power Supply Units (PSUs).
4	Hardware features	Must have redundant of other components such as fans within network equipment.
5	Hardware features	Must have redundant CPU/processor cards.
6	Hardware features	Support Redundancy for CPU cards in switching over, to allow the standby CPU to immediately take over in sub-second time scales in the event of a failure.
7	Hardware features	All components (including elements such as I/O cards, CPUs, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).
8	Hardware features	Must have minimum 4 modular slots and 2 should be dedicated for I/O modules.
9	Hardware features	For high availability & performance must have two supervisory engine
10	Hardware features	Chassis Switching Fabric Must be capable of delivering greater than 600Gbps per I/O slot. This switching speed in one direction, i.e. total of minimum 300 Gbps
11	Scalability	Chassis Must support minimum following port configuration onasked I/O modules, any of the following port configuration should be available on demand just replacing the I/O Modules: > Minimum 48 x10 Gigabit Ethernet ports > Minimum 4 x 40 Gigabit Ethernet ports
12	Scalability	Must support port channeling or equivalent across multiple chassis.
13	Scalability	Physical standards for Network Device Should support Ethernet (IEEE 802.3, 10BASE-T), Fast Ethernet (IEEE 802.3u, 100BASE-TX), Gigabit Ethernet (IEEE 802.3z, 802.3ab), Ten Gigabit Ethernet (IEEE 802.3ae)
14	Scalability	Software based standards for Network Device Must support IEEE 802.1d - Spanning-Tree Protocol, IEEE 802.1w - Rapid Spanning Tree, IEEE 802.1s - Multiple Spanning Tree Protocol, IEEE 802.1q - VLAN encapsulation, IEEE 802.3ad - Link Aggregation Control Protocol (LACP), IEEE 802.1ab - Link Layer Discovery Protocol (LLDP), IEEE 802.3x Flow Control
15	Scalability	Must support auto-sensing and auto-negotiation (Link Speed/Duplex)
16	Scalability	Routing protocol support; Static IP routing, OSPF, BGPv4, MP-BGP, BGP Route
17	Scalability	Should support Bidirectional Forwarding Detection (BFD) for OSPF, IS-IS and BGP
18	Scalability	The network infrastructure must allow for multiple equal metric/cost routes to be utilized at the same time
19	Scalability	Hardware must support FCOE ports with all FCOE standards support like FCF & DCB
20	Scalability	Must have the ability to complete hitless software upgrades with zero interruption to services or data forwarding
21	Scalability	Should support 802.1 Q-in-Q
22	Scalability	IEEE 802.3ad Link Aggregation or equivalent capabilities
23	Scalability	IPv6 functionality
24	Scalability	Must be IPv6 capable. If IPv6 compliance/support is not available, please identify if compliance is defined in device roadmap along with a timeframe
25	Scalability	IP Version 6 (IPv6) must be supported in hardware
26	Scalability	Must support Static IPv6 routing, OSPFv3
27	Scalability	Should support both IPv4 and IPv6 routing concurrently. There should be the ability to tunnel IPv6 within IPv4.
28	Scalability	Supported IPv6 features should include: DHCPv6, ICMPv6, IPv6 QoS, IPv6 Multicast support, IPv6 PIMv2 Sparse Mode, IPv6 PIMv2 Source-Specific Multicast, Multicast VPN
29	Scalability	Device must support multicast in hardware

30	Scalability	The switch mush support IEEE 802.1 QBR/ 802.1 BR standard to support scalability and extension of switching fabric to additional ports if required outside chassis.
31	Scalability	The system must allow extending Layer 2 applications across distributed data centers
32	Security features	Must support multiple privilege levels for remote access (e.g. console or telnet access)
33	Security features	Must support Remote Authentication Dial-In User Service (RADIUS) and/or Terminal Access Controller Access Control System Plus (TACACS+)
34	QoS features	Must support IEEE 802.1p class-of-service (CoS) prioritization
35	QoS features	Must support rate limiting (to configurable levels) based on source/destination IP/MAC, L4 TCP/UDP
36	QoS features	Must have the ability to complete traffic shaping to configurable levels based on source/destination IP/MAC and Layer 4 (TCP/UDP) protocols
37	QoS features	There should not be any impact to performance or data forwarding when QoS features
38	QoS features	Must support a "Priority" queuing mechanism to guarantee delivery of highest-priority (broadcast critical/delay-sensitive traffic) packets ahead of all other traffic
39	QoS features	Must support ability to trust the QoS markings received on an ingress port
40	Virtulisation	The switch must support data center virtualization, giving department the ability to virtualize a physical switch into multiple logical devices. With each logical switch having its own processes, configuration, and administration
41	Management features	Must support SNMP V1,V2, V3 and be MIB-II compliant
42	Management features	Must support SNMP traps (alarms/alerts) for a minimum of four destinations
43	Management features	Network switch should support Remote Monitoring on every port covering the following four groups (Statistics, Alarm, Event, History).
44	Management features	Must be able to integrate with all standard Network Management Systems, including HP Open View Suite, Netcool and Infovista
45	Management features	Should support flow based traffic analysis features and the ability to export of network IP flow information.
46	Management features	Must support Network Timing Protocol (NTPv3) and should support the following: • Configuration of more than one NTP server • Speciation of a local time zone • NTP authentication
47	Port requirment from Day 1	Each Core Switch should be provided with 16 x 10G Ports since Day 1
48	Support	The system should not be an end of life / end of service product.