सत्यमेव जयते

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

टेलीफोन 022 :- 3/2/1/25752040
फैक्स 35/25752029 - 022 :
ई :मेल-dgship-dgs@nic.in
वेब :www.dgshipping.gov.in

/बिटा बिल्डिंग ,वीं मंजिल99th floor, Beta Building
आई थिंक टेक्नो कैंपस/I-Think Techno Campus
कांजूर मार्ग /(पूर्व)Kanjur Marg (East)
मुंबई/MUMBAI-400 042

Tele: 022- 25752040/1/2/3
Fax: 022-25752029/35
E-mail: dgship-dgs@nic.in
Web: www.dgshipping.gov.in

No.E-Gov/NP(1)2015-VoI -I Dated : 16.11.2017

CORRIGENDUM TO TENDER NOTICE No. DGS/E-GOV/NP(1)/2015-VoI-1

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/NP(1)/2015/-VoI-1 dated 27.10.2017, the Pre-Bid Conference was held on 10.11.2017. In response to the queries received by prospective bidders, reply of the queries is enclosed as Annexure-I.

16 Nov.17

[Deependra Singh Bisen]
Asstt. Director General of Shipping

Encl: As above

CORRIGENDUM TO THE RFP FOR SELECTION OF SYSTEM INTEGRATOR FOR EGOVERNANCE SOLUTION AND IT TRANSFORMATION OF DIRECTORATE GENERAL OF SHIPPING, GOVT OF INDIA

Tender Number: DGS/E-Gov./NP(1)/2015-Vol-I

Dated: 27/10/2017

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.	I	2.1 (II)	10	The tenure of the contract of the successful bidder shall be for a term of six (6) years months ("the Term")	The tenure of the contract of the successful bidder shall be for a term of six (6) years ("the Term")
2.	I	4.9	18 19	The bidder may use the services of a sub-contractor to leverage their specialized experience in respect of following tasks/areas: i. Cloud services ii. Establishment of network infrastructure iii. Call Centre services iv. Data scanning and digitization services Sub-contracting would be subject to the following conditions: i. All sub-contracting arrangements must form part of the bid. ii. All sub-contracting contracts must be entered into by the bidder / lead bidder. iii. Sub-contracting should not dilute the responsibility and liability of the bidder. iv. Any changes in sub-contractors must be approved by DGS prior to conclusion of any contract between the bidder and the sub-contractor. v. DGS retains the right to request discontinuation of sub-contracting of activities at any time during the contract period.	The bidder may use the services of a sub-contractor to leverage their specialized experience in respect of following tasks/areas: i. Cloud services ii. Establishment of network infrastructure iii. Call Centre services iv. Data scanning and digitization services v. Training Sub-contracting would be subject to the following conditions: i. All sub-contracting arrangements must form part of the bid. ii. All sub-contracting contracts must be entered into by the bidder / lead bidder. iii. Sub-contracting should not dilute the responsibility and liability of the bidder. iv. Any changes in sub-contractors must be approved by DGS prior to conclusion of any contract between the bidder and the sub-contractor. v. DGS retains the right to request discontinuation of sub-contracting of activities at any time during the contract period.

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
3.	I	6.5 (Section C)	33, 34, 35	Cloud Service Provider Capabilities	Refer to Amended Sections 2.1 (A)
4.	I	9.1	43	Project Timelines	Refer to Amended Sections 2.1 (B)
5.	I	9.2	45 46, 47, 48	Deliverables Schedule	Refer to Amended Sections 2.1 (C)
6.	I	9.3	49	Payment Schedule	Refer to Amended Sections 2.1 (D)
7.	I	10.3 (A10)	97	Summary of Commercial Proposal	Refer to Amended Sections 2.1 (E)
8.	II	1.3.3	32	The bidder shall be responsible for procurement, supply and installation of entire IT infrastructure required for setting up and operations of the envisaged solution. The IT infrastructure includes data centre, disaster recover, networking infrastructure, internet connectivity, client side computing devices including desktops, laptops, printers, scanners, related system software, other software and any other related IT infra required for running and	The bidder shall be responsible for procurement, supply and installation of entire IT infrastructure required for setting up and operations of the envisaged solution. The IT infrastructure includes networking infrastructure, internet connectivity, client side computing devices including desktops, laptops, printers, scanners, related system software, other software and any other related IT infra required for running and operating the envisaged solution. The IT infrastructure procurement will be planned considering the below factors: A. Minimum impact to business operations continuity

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
				operating the envisaged solution. The IT infrastructure procurement will be planned considering the below factors: A. Minimum impact to business operations continuity B. Maximum availability of services to users	B. Maximum availability of services to users
9.	II	1.3.3	33	4. The ownership of IT infrastructure shall get transferred to DGS after “Acceptance and Go Live”	The ownership of IT infrastructure procured within DGS premises shall get transferred to DGS after “Acceptance and Go Live and Stabilization”
10.	II	6 (C)	85	iii. The Mobile App will allow the users with mobile devices to work on certain modules even when they are offline. It will allow users to synchronize with the system when they are back online. The SI will have to build the Mobile App with an end-to-end MAM (Mobile Application Management) functionality. The MAM solution should provide the ability to remotely: control the provisioning, updating and removal of mobile applications. The MAM should consist of features like: Single Sign On, Data Security, App usage restriction based on idle timeout, Push Services, Crash Log Reporting, App Updating, App Version Management, App Wrapping, etc.	Requirement deleted
11.	II	1.2	112	The following provides a pictorial representation of envisaged scope of work and related components for the bidder.	Refer to Amended Sections 2.1 (F)

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
12.	III	15.3	25	The liability of Bidder (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event in the aggregate exceed two (2) times average annual fees payable under this Agreement calculated over a reasonable period of months before the cause of action arose with respect to the work involved under the applicable Schedule/Annexure. The liability cap given under this Clause 15.3 shall not be applicable to the indemnification obligations set out in Clause 15.1 and breach of Clause 12.4 and 17.	The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement. The liability cap given under this Clause 15.3 shall not be applicable to the indemnification obligations set out in Clause 15.1 and breach of Clause 12.4 and 17.
13.	III	19.3	32, 33	Pre-existing work: For the purpose of this Agreement, ‘pre-existing work’ shall mean such pre-existing work of bidder and that of its subcontractors, agents, representatives: i. that were identified by the bidder in its Proposal ii. for which bidder had provided sufficient documentary proof to establish that such work belongs solely to bidder (or its subcontractors, agents, representatives) iii. which were accepted by DGS (based on the documentary proof) as pre-existing work of bidder. To the extent bidder uses any of pre-existing work of the bidder (or its subcontractors, agents, representatives) in provision of services/	Pre-existing work: For the purpose of this Agreement, ‘pre-existing work’ shall mean such pre-existing work of bidder and that of its subcontractors, agents, representatives: i. that were identified by the bidder in its Proposal ii. for which bidder had provided sufficient documentary proof to establish that such work belongs solely to bidder (or its subcontractors, agents, representatives) iii. which were accepted by DGS (based on the documentary proof) as pre-existing work of bidder. All IPR including the source code and materials developed or otherwise obtained independently of the efforts of a Party under this Agreement (“pre-existing work”) including any enhancement or modification thereto shall remain the sole property of that Party. During the performance of the services for this agreement, each party grants to the other party (and their subcontractors

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
				Deliverables under this Agreement, the bidder hereby transfers (for itself and on behalf of its subcontractors, etc.) all rights, title and interest (including all intellectual property rights) for the customization / development that happens on such pre-existing work to DGS. Bidder shall provide to DGS (to the satisfaction of DGS) all documentation including, without limitation, source code, object code, SRS, FRS, operational documents etc. for the customization / development that happens on such pre-existing work.	as necessary) a non-exclusive license to use, reproduce and modify any of its pre-existing work provided to the other party solely for the performance of such services for duration of the Term of this Agreement. Except as may be otherwise explicitly agreed to in a statement of services, upon payment in full, the Implementation Agency should grant Purchaser a non-exclusive, perpetual, fully paid-up license to use the pre-existing work in the form delivered to Purchaser as part of the service or deliverables only for its internal business operations. Under such license, either of parties will have no right to sell the pre-existing work of the other party to a Third Party. Purchaser's license to pre-existing work is conditioned upon its compliance with the terms of this Agreement and the perpetual license applies solely to the pre-existing work that bidder leaves with Purchaser at the conclusion of performance of the services.
14.	III	6.0	71	Leveraged Document management software should figure in the Leader/Challenger Quadrant of Gartner Magic Quadrant or Leader/Strong Performer in Forrester's Wave or Classified as leaders as per latest IDC MarketScape in the last one year as on day of submission of bid	Leveraged Document management software should figure in the Leader/Challenger Quadrant of Gartner Magic Quadrant or Leader/Strong Performer in Forrester's Wave or Classified as leaders as per latest IDC MarketScape in the last one year as on day of submission of bid Or Leveraged Document management software should be successfully implemented in atleast 5 Central / State Govt Organizations in India in last 5 years. The same should be supplemented with Go-Live certificates from Client. Without Client Certificate, proposed Document Management Software will not be considered as compliant solution. Bidder specific case studies or certification will not be considered.
15.	III	7.0	73	Application should ensure Compatibility with all platforms such as Windows, Google Android, & Apple iOS etc.	Application should ensure Compatibility with all platforms such as Google Android,& Apple iOS etc.

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
16.	III	1.11.3	84	The cap of 10% as mentioned above will not be applicable in both cases 1.7.1 and 1.7.2.	The cap of 10% as mentioned above will be applicable in both cases 1.7.1 and 1.7.2.
17.	Annexure 1	6.0 Document Management System	71	37. The solution should support single metadata store for modules such as Document Management, Web Content Management, Records Management and Digital Asset Management.	The solution should support single metadata store for modules such as Document Management, Web Content Management, etc.
18.	Annexure 2	Technical Specifications	78, 79, 80	Technical Specifications	Refer to Amended Sections 2.1 (G)
19.	Annexure 2	Technical Specifications	78 - 123	Technical Specifications 3. Managed Access Switch, 14. Intranet Router, 15. Internet Router, 16. Core Switch	Requirements Deleted Refer to Amended Sections 2.1 (G)
20.	Annexure 2	8. enterprise management system	98	167. The proposed Asset Management solution must be able to collect WBEM information. 180. It should allow host enabled recording which allows the end user to initiate a recording session. 181. 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.	Requirements Deleted

Sr. No.	Volume	Section / Clause	Page No.	Original Clause	Amended Clause
				184. It should support remote Reboot & Chat functions between nodes.	
21.	Annexure 3	Indicative Bill of Material	125	1.1 Central System	Refer to Sections 2.1 (H)

2 Amended Sections

2.1 Amended Sections of RFP Volume I

A. Section 6.5 – Technical Bid Evaluation

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

C	**Cloud Service Provider Capabilities**	**1000**	
C.1	Credentials of Cloud Service Provider: Bidder/**Cloud Service Provider** with maximum numbers of active clients in proposed Data Center be awarded full marks and the others shall be awarded marks on relative (pro-rata) basis.	200 Marks	The bidder/**Cloud Service Provider** is required to self-certify on their company letter head by Authorized Signatory regarding active clients in proposed Data Center
C.2	Tier Classification of the proposed Data Center, where cloud hosting is to be served from Tier III / Tier IV : 200 Marks < Tier III : 0 Marks	200 Marks	Copy of valid certification, mentioning exact tier type and location
C.3	Tier Certification of Operational Sustainability Bronze : 100 Silver : 150 Gold : *200*	200 marks	Copy of valid certification
C.4	Multiple Data Centers: Bidder/**Cloud Service Provider** with maximum numbers of data centers in different seismic zones will be awarded full marks and the others shall be awarded marks on relative (pro-rata) basis.	150 Marks	The bidder/ **cloud service provider** is required to self-certify on their company letter head by Authorized Signatory regarding numbers of data centers in different seismic zones
C.5	Number of Certified Data Center Professionals (CDCP certified) Marks will be awarded as below :	150 Marks	Certificate from HR head of bidder/**cloud service**

	○ >= 5 – 50 Marks ○ 5 to 10 – 100 Marks ○ 10 to 20 – 150 Marks ○ >25 – 200 Marks		**provider** along with the list of certified staff members
C.6	The Bidder / **Cloud Service Provider** should have experience in setting-up cloud solution in India during the last Seven years. Cloud Solution set-up would mean where the Bidder/**Cloud Service Provider** has, procured, installed and commissioned Cloud Infrastructure (Hardware and Software). **50 marks per project (Maximum 2 projects)**	100	Copy of work order and Completion Certificate from the client; OR Copy of work order and Self Certificate of Completion (Certified by CS/independent auditor of the bidding entity); OR Copy of work order and Phase Completion Certificate (Certified by Client OR CS/independent auditor of the bidding entity); **Note:** For International projects, the bidder/**cloud service provider** has to provide copy of purchase order along with a case study of the project.

B. Section 9.1 – Project Timeline

Activity Code (1.5) and Track (1.24) in the section 9.2 of Volume I will 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 + 7 months**	D5
1.6	CDC	Specifications for required Cloud Data Centre and Disaster Recovery Centre	T + 2 months	D6
1.7	CDC	Completion of Cloud DC and DR	T + 7 months	D7
1.8	NWI	Specifications for networking infrastructure	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 + 9 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 + 9 months	D13

Activity code	Track	Description	Timeline	Acceptance criteria
1.14	CMT	Data migration plan	T + 1 months	D14
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 + 9 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 + 9 months	D22
1.23	All	Successful completion of parallel run with existing system	T + 12 months	D23
1.24	**DSD**	Setup of data scanning services for DGS operations & commencement of data scanning activities	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	CRT	STQC Certification	T + 8	D27
Phase 2 - Operations and maintenance phase				

Activity code	Track	Description	Timeline	Acceptance criteria
2.1	ONM	Operations and maintenance of the entire solution for a period of 5 years after stabilization	T1 + 60 months	D28

C. Section 9.2 – Deliverables

Deliverables (D21, D24, and D26) in the section 9.2 of Volume I will 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	T + 3 months

Deliverables	Deliverable Description	Expected Timelines
	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	
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
D6	Cloud Data centres establishment report should cover the following: - Specifications & Design of Cloud DC & DRC - Installation & Commissioning of Cloud DC & DRC detailed plan	T + 2 months
D7	Report on Cloud DC & DR readiness should cover the following: - Commissioning of Cloud DC & DR	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 + 9 months

Deliverables	Deliverable Description	Expected Timelines
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 + 9 months
D14	Data migration report should cover the following: - Data migration assessment - Migration & transitioning approach - Detailed data migration plan	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 + 9 months
D18	Data migration completion report should cover the following: - Details of actual data that has been migrated - Certificate from DGS officials confirming successful completion of data migration	T + 9 months
D19	Establishment of IT facilities management system should cover the following:	T + 9 months

Deliverables	Deliverable Description	Expected Timelines
	- Report on Operationalization of Help desk - Standard Operating Procedures and Operations Manuals - Obtaining Relevant Certifications	
D20	Scanning & Digitization procedures & specification report should cover the following: - Requirements gathering of scanning & digitization of DGS - Detailed plan of scanning & digitization	T + 1 months
D21	Scanning & Digitization readiness report should cover the following: - Status of scanning & digitization - Details of completion of activities **- Standard Operating manuals of scanning & digitization**	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 + 9 months
D23	Certification of successful completion of parallel run	T + 12 months
D24	-Certification of setup of data scanning services & commencement report **-Scripts required for importing data that has been migrated**	T + 3 months
D25	Certification of SLA monitoring system - Third party agency should certify SLA monitoring system	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 **Report on Completion of Data Scanning and Digitization**	T1 = T + 12 months
D27	STQC report and Certificate	T+8
D28	SLA Compliance Reports (Monthly) should cover the following: - Performance Monitoring reports for system	T1 + 60 months

Deliverables	Deliverable Description	Expected Timelines
	- 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	

D. Section 9.3 – Payment Schedule

Payment Schedule for deliverables and other payments in the section 9.3 of Volume I will be read as follows

Phase	Deliverable	Payment Amount	Expected Timeline	Deliverable no.
Phase I	Acceptance of Project charter, Scanning & Digitization procedure & specification report and Data migration report	20% of Y , against submission of additional PBG of equivalent amount valid for 30 days beyond Go-Live date	T + 1 months	D2, D14, D20,
Phase I	Software requirement Specification document, Data center establishment report, Network infrastructure establishment report, Client side computing establishment report and Scanning & Digitization readiness report	10 % of Y	T + 2 months	D3, D6, D8, D11, D21
Phase I	Acceptance of UAT – “Client side computing set up completion report” and “**Change Management & Training completion report” for UAT**	5% of Y	T + 7 months	**D12, D16**
Phase I	Acceptance of Go Live – “Client side computing set up	5% of Y	T + 9 months	D5, D10, D13

	completion report" and Network infrastructure set-up completion for Go Live report along with Acceptance of Software Deployment report			
Phase I	Certification of successful completion of parallel run – Go Live	20 % of Y	T + 12 months	D23
Phase II	Quarterly payment for next 5 years	2% of Y	T +60	D28

Other Payments				
Phase	**Deliverable**	**Payment Amount**	**Payment terms**	**Deliverables**
Payment Schedule for client side hardware and related computing				
Phase I	Client side hardware delivery	60% of A2	Total Pay-out will not exceed 100% of total quoted cost (A2)	D12
Phase I	Client side hardware installation	30% of A2		D13
Phase I	Go Live	10% of A2		D26
Phase II	Operations and Maintenance	5% - 20 Equal quarterly payment for next 5 year	Total Pay-out will not exceed 100% of total quoted cost (A9.1.2)	
Cloud DC and DR				
Phase II	Cloud DC and DR	5% - 20 Equal quarterly payment for next 5 year	Quarterly payments on usage basis, after deducting all applicable penalties. Total Pay-out will not exceed 100% of total quoted cost (X3)	D6+D7
Scanning & Digitization				

Phase I & Phase II	Scanning and Digitization & Data Entry	On actuals	**Quarterly payments on usage basis, after deducting all applicable penalties. Total Pay-out will be based on actuals as per the unit rate quoted by the bidder in the commercial proposal.**	D20 + D21
SMS Gateway				
Phase I & Phase II	SMS Gateway usage	On actuals	**Quarterly payments on usage basis, after deducting all applicable penalties. Total Pay-out will be based on actuals as per the unit rate quoted by the bidder in the commercial proposal.**	D22
Network Infrastructure				
Phase I	Network Infrastructure setup completion for UAT	60 % of A3	Total Pay-out will not exceed 100% of total quoted cost (A3)	D9
	Network Infrastructure setup completion for Go-Live	40 % of A3		D10
Phase II	Operations and Maintenance	5% - 20 Equal quarterly payment for next 5 year	Total Pay-out will not exceed 100% of total quoted cost (A9.1.3)	D9 +D10

E. Comp1: Summary of Commercial Proposal

The Summary for Scanning & Digitization will be read as follows

A10: Scanning and Data Digitization services

Data Entry

Sr. No.	**Description**	**Quantit y (A10.1)**	**Rate (A10.2)**	**Period (A10.2.1)**	**Total Price (Rs.) A10.3 =(A10.1 * A10.2*A10.2.1)**
1.	Data Entry operators (minimum 5 resources)				

Total data entry fields (approximately)	**6,00,00,000**

Scanning & Digitization

Sr. No.	**Description (Size of the document)**	**Quantity (A10.4)**	**Rate (A10.5)**	**Total Price (Rs.) A10.6 =(A10.4 * A10.5)**
1	A0			
2	A1			
3	A2			
4	A3			
5	A4			
6	Legal			
TOTAL (A10.7)				

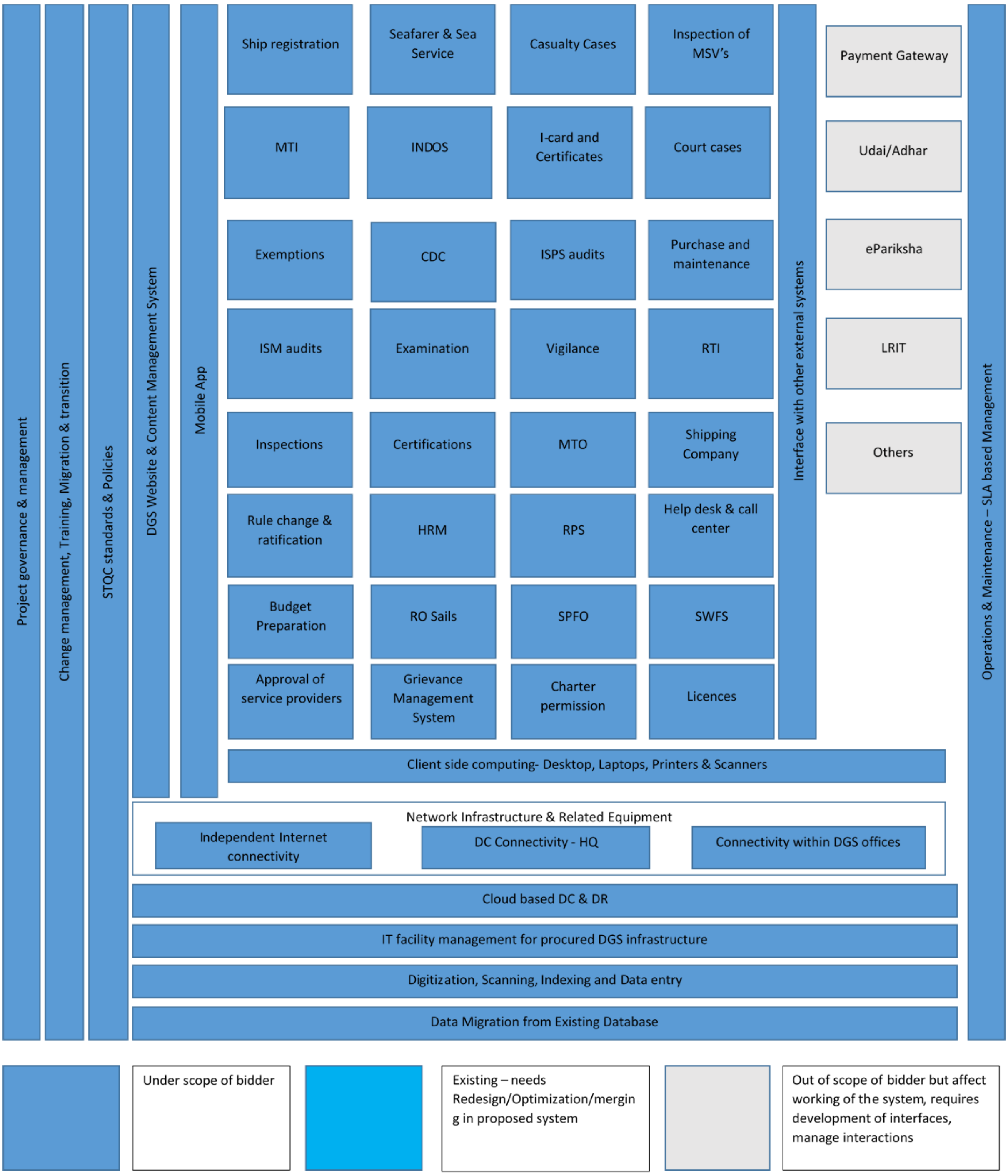
Total pages to be scanned	**1,00,00,000**

Tax: Against A10 component

Subtotal (A10.3) and (A10.7)	Tax	Tax rate	Tax amount	Total A10 = (A10.3 + A10.7 + Tax amount)
	CGST			
	SGST			
	IGST			
	Any other tax			
Total (in Figures) (A10)				
Total (in Words) (A10)				

F. Pictorial representation of envisaged scope of work and related components for the bidder

Schematic representation of bidder’s scope of work will be read as follows


Project governance & management
Change management, Training, Migration & transition
STQC standards & Policies
DGS Website & Content Management System
Mobile App
Ship registration
Seafarer & Sea Service
Casualty Cases
Inspection of MSV’s
MTI
INDOS
I-card and Certificates
Court cases
Exemptions
CDC
ISPS audits
Purchase and maintenance
ISM audits
Examination
Vigilance
RTI
Inspections
Certifications
MTO
Shipping Company
Rule change & ratification
HRM
RPS
Help desk & call center
Budget Preparation
RO Sails
SPFO
SWFS
Approval of service providers
Grievance Management System
Charter permission
Licences
Interface with other external systems
Payment Gateway
Udai/Adhar
eParIksha
LRIT
Others
Operations & Maintenance – SLA based Management
Client side computing- Desktop, Laptops, Printers & Scanners
Network Infrastructure & Related Equipment
Independent Internet connectivity
DC Connectivity - HQ
Connectivity within DGS offices
Cloud based DC & DR
IT facility management for procured DGS infrastructure
Digitization, Scanning, Indexing and Data entry
Data Migration from Existing Database
Under scope of bidder
Existing – needs Redesign/Optimization/mergin g in proposed system
Out of scope of bidder but affect working of the system, requires development of interfaces, manage interactions

G. Annexure 2 – Technical Specifications

Technical Specification for 1, 2, 10 and 15 to 21 in the Annexure 2 will be read as follows

MAF			
#	**Components**	**Submitted**	**Document Reference**
1	Desktop		
2	Laptop		
3	Cloud Data Center hosting specifications (Servers, Storage etc.)		
4	Cloud DC & DR Server Security Services		
5	Cloud Network security Services		
6	Cloud Application and Platform Services		
7	Enterprise Management System		
8	Multi-function Printer		
9	UPS		
10	Firewall Services		
11	IPS Services		
12	Optical Fibre Cable		
13	DDOS Services Cloud DC & DR		
14	Antivirus Services for Cloud DC & DR		
15	Web Application Firewall Services		
16	HIPS Service		
17	Anti APT Service		
18	BCM Service		
19	Router		
20	Access Switch 24 Port		
21	Access Switch 8 Port		

1.DESKTOP					
#	**Nature of Requirement**	**Minimum Requirement Description for Desktop**	**Compliance (Y/N)**	**Reasons for Deviation (if any)**	**Details**
1	CPU	Intel or AMD			
2	Processor	Intel **Core i5** or Higher and for AMD A10 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 or higher professional 64 bit OS.**			
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 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. 4 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			
19	**Software**	**MS- Office Latest Version**			

2.LAPTOP

#	Nature of Requirement	Minimum Requirement Description for Laptop	Compliance (Y/N)	Reasons for Deviation (if any)	Details
1	Processor	Intel 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	1 TB@ HDD 7200 RPM			
5	HDD Controller	Integrated dual port SATA-II controller			
6	Operating System	**Preloaded with latest windows 8 or higher professional 64 bit OS**			
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			
16	**Software**	**MS - Office Latest Version**			

10. Firewall Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
1	Solution/offering would be a cloud-based Firewall service.			
2	The Firewall Appliance / solution / offering should have certifications like NDPP / ICSA / EAL4 or more.			
3	The Appliance / virtual /cloud offering based security platform should be capable of providing firewall, IPS, and VPN (both IPSec and SSL) functionality in a single appliance			
4	The Appliance / virtual /cloud offering hardware should be a multicore CPU architecture with a hardened operating system to support higher memory			

10. Firewall Services				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
5	Proposed Firewall should be open/ ASIC architecture based on multi-core cpu's to protect & scale against dynamic latest security threats.			
6	Firewall should support atleast sufficent concurrent VPN peers IPSec / SSL			
7	Firewall should support minimum vlans as required in the project			
8	Firewall should support virtual firewalls from day one & support licensed based scalability as & when required			
9	Firewall should provide application inspection for DNS, FTP, HTTP, SMTP,ESMTP, LDAP, VLAN, VXLAN, MGCP, RTSP, SIP, SCCP, SQLNET, TFTP, H.323, SNMP			
10	Should be able to group multiple firewalls together as a single logical device and should scale performance in term of combined throughput, connections and connections per second			
11	Firewall should support creating access-rules with IPv4 & IPv6 objects			
12	Firewall should support operating in routed & transparent mode. Should be able to set mode independntly for each context in multi-context mode			
13	In transparent mode firewall should support arp-inspection to prevent spoofing at Layer-2			
14	Should support Non Stop Forwarding in HA during failover and Graceful Restart			
15	Firewall should support static nat, pat, dynamic nat, pat & destination based nat			
16	Firewall should support Nat66 (IPv6-to-IPv6), Nat 64 (IPv6-to-IPv4) & Nat46 (IPv4-to-IPv6) functionality			
17	Firewall should support Restful API for integration with 3rd party solutions like Software Defined Networking			
18	Firewall should support stateful failover of sessions in Active/Standby or Active/Active mode			

10. Firewall Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
19	Firewall should support etherchannel functionality for the failover control & date interfaces for provide additional level of redundancy			
20	Firewall should support redundant interfaces to provide interface level redundancy before device failover			
21	Firewall should support 802.3ad Etherchannel functionality to increase the bandwidth for a segment across different modules			
22	Firewall should support failover of IPv4 & IPv6 sessions			
23	Firewall should replicate Nat translations, TCP,UDP connection states, ARP table, ISAKMP & IPSec SA's, SIP signalling sessions			
24	Firewall should have integrated redundant power supply			
25	Firewall should support client based and clientless SSL vpn peers from day one.			
26	Firewall should support RFC 6379 based Suite-B Cryptography Suites/algorithms like AES-GCM/GMAC support (128-, 192-, and 256-bit keys), ECDH support (groups 19, 20, and 21), ECDSA support (256-, 384-, and 521-bit elliptic curves) for enhanced VPN security.			
27	Firewall should support latest IKEv2 standards for supporting SHA-2 256, 384 & 512 bit message integrity algorithms in hardware to ensure there is no performance bottleneck & higher security.			
28	Firewall should support RFC 6379 based Suite-B Cryptography Suites/algorithms like AES-GCM/GMAC support (128-, 192-, and 256-bit keys), ECDH support (groups 19, 20, and 21), ECDSA support (256-, 384-, and 521-bit elliptic curves) for enhanced VPN security.			

10. Firewall Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
29	The proposed solution should be VPNC/ICSA compliant for interoperability.			
30	Should support pre-shared keys & Digital Certificates for VPN peer authentication			
31	Should support perfect forward secrecy & dead peer detection functionality			
32	Should support Nat-T for IPSec VPN			
33	Routing Features			
34	Firewall should support IPv4 & IPv6 static routing, RIP, OSPF v2 & v3, PBR, VLAN, VXLAN for PBR, PBR for IPv6 BGP and BGPv6			
35	Firewall should support PIM multicast routing			
36	Firewall should support SLA monitoring for static routes			
37	Firewall should support management of firewall policies via Cli, SSH & inbuilt GUI management interface.			
38	Firewall should support SNMP v1,2c & 3 simultaneously			
39	Firewall should support packet capturing functionality			
40	Firewall should support the functionality of Auto-Update to check for latest software versions & download the same			

15. Web Application Firewall Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
1	Solution/offering would be a cloud-based Web Application Firewall services			

15. Web Application Firewall Services				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
2	The Web application firewall should address Open Web Application Security Project (OWASP) Top Ten security vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Broken Authentication, Session Management etc.			
3	The solution should prevent the following attacks (but not limited to):			
	a) Brute force /DDOS			
	b) Access to predictable resource locations			
	c) Unauthorized navigation			
	d) Web server reconnaissance			
	e) HTTP request format and limitation violations (size, unknown method, etc.)			
	f) Use of revoked or expired client certificate			
4	Should support positive and negative security model.			
5	Should have the ability of caching, compression of web content and SSL acceleration.			
6	Should have integrated SSL Offloading capabilities, further the solution should support SSL and/or TLS termination, or be positioned such that encrypted transmissions are decrypted before being inspected by the WAF.			
7	Should have integrated basic server load balancing capabilities.			
8	Bidder should have the ability to inspect web application output and respond (allow, block, mask and/or alert) based on the active policy or rules, and log actions taken.			
9	Bidder should inspect both web page content, such as Hypertext Markup Language (HTML), Dynamic HTML (DHTML), and Cascading Style Sheets (CSS), and the underlying protocols that deliver content, such as Hypertext Transport Protocol			

15. Web Application Firewall Services				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
	(HTTP) and Hypertext Transport Protocol over SSL (HTTPS). (In addition to SSL, HTTPS includes Hypertext Transport Protocol over TLS.)			
10	WAF should support dynamic source IP blocking and should be able to block attacks based on IP source.			
11	Should inspect XML in addition to HTTP (HTTP headers, form fields, and the HTTP body).			
12	Inspect any web socket protocol (proprietary or standardized) or data construct (proprietary or standardized) that is used to transmit data to or from a web application, when such protocols or data are not otherwise inspected at another point in the message flow.			
13	WAF should support inline bridge or proxy mode of deployment.			
14	WAF should have an option to configure in Reverse proxy mode as well.			
15	Actions taken by WAF to prevent malicious activity should include the ability to drop requests and responses, block the TCP session, block the application user, or block the IP address.			
16	Transactions with content matching known attack signatures and heuristics based should be blocked.			
17	The WAF database should include a preconfigured comprehensive and accurate list of attack signatures.			
18	The Web application firewall should allow signatures to be modified or added by the administrator.			
19	The Web application firewall should support automatic updates (if required) to the signature database, ensuring complete protection against the latest application threats.			

15. Web Application Firewall Services				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
20	WAF support the following normalization methods:			
21	a) URL-decoding (e.g. %XX)			
	b) Null byte string termination			
	c) Self-referencing paths (i.e. use of /. / and encoded equivalents)			
	d) Path back-references (i.e. use of /.../ and encoded equivalents)			
	e) Mixed case			
	f) Excessive use of whitespace			
	g) Comment removal (e.g. convert DELETE/**/FROM to DELETE FROM)			
	h) Conversion of (Windows-supported) backslash characters into forward slash characters.			
	i) Conversion of IIS-specific Unicode encoding (%uXXYY)			
	j) Decode HTML entities (e.g. c, ", ª)			
	k) Escaped characters (e.g. \t, \001, \xAA, \uAABB).			
22	WAF should support different policies for different application sections.			
23	The Web application firewall should automatically learn the Web application structure and elements.			
24	The Web application firewall learning mode should be able to recognize application changes as and when they are conducted.			
25	The WAF should have the ability to perform behavioral learning to examine traffic and highlight anomalies and provide recommendations that can be turned into actions such as apply, change and apply, ignore etc.			
26	The Web application firewall should support line speed throughput and minimal latency so as not to impact Web application performance.			
27	For SSL-enabled Web applications, the certificates and private/public key pairs for the Web servers being			

15. Web Application Firewall Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
	protected need to be up loadable to the Web application firewall.			
28	The Web Application Firewall should have "anti-automation" protection which can block the automated attacks that use hacking tools, scripts, frame work etc.			
29	The Web application firewall should have an out of band management port.			
30	The Web application firewall should support web based centralized management and reporting for multiple appliances.			
31	Bidder should be able to deploy the Web application firewall and remove the Web application firewall from the network with minimal impact on the existing Web applications or the network architecture.			
32	The Web application firewall should be able to generate custom or pre-defined graphical reports on demand or scheduled.			
33	The Web application firewall should provide a high level dashboard of system status and Web activity.			
34	Should be able to generate comprehensive event reports with filters:			
	a. Date or time ranges			
	b. IP address ranges			
	c. Types of incidents			
	d. Geo Location of attack source			
35	The following report formats are deemed of relevance: Word, RTF, HTML, PDF, XML, etc.			
36	Unique transaction ID should be assigned to every HTTP transaction (a transaction being a request and response pair), and included with every log message.			
37	Access logs can periodically be uploaded to the logging server if			

15. Web Application Firewall Services				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
	required (e.g. via FTP, SFTP, WebDAV, or SCP).			
38	Web application firewall should provide notifications through Email, Syslog, SNMP Trap, Notification via HTTP(S) push etc.			
39	WAF should be able to log full session data once a suspicious transaction is detected.			
40	Should be simple to relax automatically-built policies.			
41	The solution should provide the admin to manually accept false positives.			
42	Should be able to recognize trusted hosts.			
43	The WAF in passive mode should be able to provide impact of rule changes as if they were actively enforced.			
44	Should support clustered deployment of multiple WAFs sharing the same policy.			
45	The solution should support virtual environments.			
46	The solution should have the capability of load balancing between the applications in an active – active environment.			
47	The Web application Firewall should support authentication with LDAP and radius server.			
48	The Solution should allow troubleshooting issues using commands like PING, trace route, etc.			
49	The Solution should have option to configure NTP server details.			
50	Should support both IPv4 and IPv6			

16. Component: HIPS Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
1	Solution/offering would be a cloud-based service			
2	The solution should enable threat detection, identification, and prevention.			
3	The solution should analyzes all packets to and from the servers /VM's for intrusion attempts and propagation.			
4	The solution should encompasses host-based firewall capability. Must allow definition of network-level filtering rules based on source and destination IP/network address, protocol, and source and destination ports in support of organizational security policy to allow/disallow specific types of activity between hosts.			
5	The solution should have the option to apply time based firewall policy.			
6	Administrator can schedule the time of day or week when the policy will be applicable.			
7	The solution should combine NIPS (network) and HIPS (host) based signature to proactively protect against intrusion targeted at the servers.			
8	The solution should support adaptive mode to automatically learn rules.			
9	The solution should use vulnerability based and not exploit based signatures. It should detect and block all known, high risk exploits along with their underlying vulnerability (not just one exploit of that vulnerability).			
10	The solution should provide protection for Web Server and Database Server.			
11	The solution should protect Web applications by inspecting SSL-encrypted HTTP traffic streams before they reach the application.			

16. Component: HIPS Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
12	The solution should protect against SQL injection attacks.			
13	The solution should protect against cross-site scripting (XSS) attacks.			
14	The solution should support system lock-down by blocking all the applications to run on the system. The administrator can create a white list of application so that only those applications are allowed to be executed.			
15	The solution should encompass a wide array of built-in alerting, blocking, and logging responses for each event.			
16	The solution should support response adjustment on a per signature basis.			
17	The solution should support various actions such as play sound, capture trace, flash tray icon, email alert etc.			
18	The solution should have the option to block intruder for a particular period of time.			
19	The agents shall be managed by a central administration system designed for large-scale enterprise deployments.			
20	The solution should support a wide variety of reports. Should be able to generate report data into a variety of different file formats like HTML, PDF etc.			

17. Component: Anti APT Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
1	Solution/offering would be a cloud-based Anti APT Service			

17. Component: Anti APT Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
2	The proposed solution should be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, drive by download, watering hole and targeted Advanced Persistent Threat without relying on just Signature database.			
3	The proposed solution should be able to perform dynamic real-time analysis of advanced malware on the appliance itself to confirm true zero-day and targeted attacks. No information should be sent to third party systems or cloud infrastructure system for analysis and detection of Malware.			
4	The proposed solution should be able to automatically detect and confirm multistage zero day malware and targeted attacks without prior knowledge of the malware.			
5	The proposed solution should be able to utilize a state-full attack analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack, from system exploitation to outbound malware communication protocols leading to data exfiltration.			
6	The proposed solution should analyze advanced malware against a cross-matrix of different operating systems and various versions of pre-defined applications.			
7	The proposed solution should have the ability to analyze, detect and block malware in common file formats including but not limited to executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives,			

17. Component: Anti APT Services				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
	3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm, Hanword (HWP, HWT) to prevent advanced Malware and Zero-day attacks.			
8	The proposed solution should capture and store packet captures of traffic relevant to the analysis of detected threats.			
9	The proposed solution should have the ability to display the geo-location of the remote command and control server(s) when possible.			
10	The proposed solution should have the ability to report the Source IP, Destination IP, C&C Servers, URL, BOT name, Malware class, executable run, used protocols and infection severity of the attack.			
11	The proposed solution should be able to send both summary notifications and detailed per-event notifications utilizing the protocols (SMTP, SNMP, or HTTP POST) and standard formats (e.g. JSON and XML).			
12	The proposed solution should have the ability to be deployed in the following modes: out-of-band mode, inline monitoring mode, inline active blocking mode etc.			
13	The proposed solution should have fail-open capability to allow all packets to pass through the sub-system in case of software, hardware or power failure when it is deployed inline.			
14	The proposed solution should be capable to block inbound malicious exploits delivered via a web channel and outbound call-			

17. Component: Anti APT Services				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
	back communications when deployed in inline, or out-of-band mode.			
15	The proposed (file malware protection) solution should have the ability to be deployed in the following modes; on-demand scanning and continuous scanning.			
16	The proposed solution should be able to support both Selective file scanning and off box scanning of hard drive for advanced malware threats.			
17	The solution must be able to perform a pre-assessment scan of the file server offering information about the files hosted on the server.			
18	The proposed solution should be able to scan servers that support CIFS and NFS protocol for sharing and transferring files.			
19	The proposed solution should provide ability to create a quarantine share and move malicious files to that share as well as the ability to create a good share and the ability to move clean files to that share.			
20	The proposed solution should provide visibility into scan histories of each file scanned that are aborted, completed, or in progress. Logs should be able to be opened in a spreadsheet tool (once you save them in comma-separated or CSV format) if you want to view them in a spreadsheet.			
21	The proposed solution should be able to analyse saved email (e.g-.eml) files by parsing and analysing them for malicious attachments, and quarantines them if any of the attached files are found to be malicious.			

17. Component: Anti APT Services				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
22	The solution should support for SIEM log integration.			
23	The solution should be able to schedule reports and also provide the flexibility to generate on-demand reports like daily/weekly/monthly/ yearly/specific range (day and time) etc.			
24	The solution should be able to inspect and block all network sessions regardless of protocols for suspicious activities or files at various entry/exit sources to the network.			
25	The solution should be able to work in inline mode and protect against Advanced Malware, zero-day web exploits and targeted threats without relying on signature database.			
26	The solution should be able to identify malware present in network file shares and web objects (EXE, DLL, PDF, Microsoft Office Documents) Java (.jar and class files), embedded objects such as JavaScript, Flash, images etc. , compressed (zip) and encrypted (SSL) content.			
27	The solution should be able to block malware downloads over different protocols.			
28	The solution should have Sandbox test environment which can analyze threats to various operating systems, browsers, databases etc.			
29				
30	The solution should be able to detect and prevent bot outbreaks including identification of infected machines.			
31	The solution should be appliance based with hardened OS. No information should be sent to third			

17. Component: Anti APT Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
	party systems for analysis of malware automatically.			
32	The solution should be able to block the call back tunnel including fast flux connections.			
33	The solution should be able to capture packets for deep dive analysis.			
34	The solution should be able to pinpoint the origin of attack.			
35	The solution should be able to conduct forensic analysis on historical data.			
36	Dashboard should have the feature to report Malware type, file type, CVE ID, Severity level, time of attack, source and target IPs, IP protocol, Attacked ports, Source hosts etc.			
37	The solution should generate periodic reports on attacked ports, malware types, types of vulnerabilities exploited etc.			
38	The solution should be able to export event data to the SIEM or Incident Management Systems.			
39	Solution should be able to monitor encrypted traffic.			
40	The management console should be able to provide information about the health of the appliance such as CPU usage, traffic flow etc.			
41	The solution should display the geo-location of the remote command and control server.			
42	The solution should be able to integrate with Active Directory / LDAP to enforce user based policies.			

18. Component: BCM Services

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
1	The cloud provider must set up and operate a business continuity management system			
2	The bidder must make the prioritising of the restart for the cloud services provided transparent to their customers			
3	Regular business continuity management exercises (e.g. in the closing down of a Cloud Computing location)			
4	The bidder should provide evidence that their business continuity management system is based on an internationally recognised standard such as BS 25999 or ISO 22301			

19. Component: Router				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
1	The router should support IP routing, IP multicast, QoS, IP mobility, multiprotocol label switching (MPLS), VPNs and internal power supply.			
2	Router should have minimum 4 GB of of DRAM/RAM and 4GB Flash. Should support increasing of flash/compact flash size to hold multiple image, data, debugs etc.			
3	Router should have a) 2- Ports 10/100/1000 onboard RJ-45 based WAN ports b) Minimum 1 or more 1GE SFP ports.			

4	Routers should have at least 2 sFP ports for LAN / WAN. Router must have a) 2-Ports Serial WAN Interface Card with V35 cables b) 4 x 10/100/1000 LAN ports Router shoud have support for E1/ Channelized E1, Serial V.35, G.703, LTE			
5	The router performance should be scalable upto 300 Mbps or more			
6	The router shall support adaptive routing adjustments by doing routing path selection based upon advanced criteria like Response time, packet loss, delay, jitter and traffic load to intelligently control the traffic to maximise the quality of the user experience.			
7	Routers should support marking, policing and shaping			
8	IPv4 and IPv6 enabled from day one			
9	HSRP/VRRP, Static Routes, RIPv1, RIPv2, RIPng, OSPFv2, OSPFv3, BGP4, MBGP, BGp route reflector, BFD, Policy based routing IGMP V1/V2/V3, PIM-DM, PIM-SM enabled from day one			
10	Should support extensive support for SLA monitoring, alerts for metrics like delay, latency, jitter, packet loss			
11	Support for accounting of traffic flows for Network planning and Security purposes			
12	Routers should support Software upgrades			

13	Routers should support SNMPv2 and SNMPv3, Extensive Debugs			
14	Shall support Secure Shell for secure connectivity			
15	Should have to support Out of band management through Console and an external modem for remote management			
16	Pre-planned scheduled Reboot Facility			
17	The Router should be NDPP or EAL3 certified at the time of Bidding			
18	Router should have DES, 3DES and AES Standards through dedicated encryption module/processor. Should support IPSec with IKEv2 and Suite-B Encryption			
19	Router should have Vrf aware stateful Firewall Inspection features			
20	Router should support monitoring of network traffic with application level insight with deep packet visibility into web traffic using flow analysis cRTP or equivalent			
21	Must support dynamic Mesh IPsec tunnel solution without having to pre-configure all tunnel end-point peers or equivalent. Must support VPN solution based on RFC3547 - Group Domain of Interpretation (GDOI) or equivalent feature/protocol, Generic Routing Encapsulation RFC 1701/2784/2890) and /RFC 2332 (next-hop resolution protocol)			

20. Component: Access Switch 24 Port				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
Layer 2- (24Port) Switch				
1	Architecture			
1.1	Shall be 1RU, 19" Rack Mountable			
1.2	24 RJ-45 autosensing 10/100/1000 ports			
1.3	The switch shall support up to two 1/10-Gigabit ports (SFP+) in addition to the above ports			
1.4	1 RJ-45 serial console port			
1.5	128 MB SDRAM and 16 MB flash			
1.6	Shall have switching capacity of 120 Gbps "minimum.			
1.7	Shall have up to 95 mpps pps switching throughput			
2	Resiliency			
2.1	Switch should support stacking so as to operate as one unit			
2.2	Switch should support stacking so as to operate as one unit			
2.3	Shall support redundant power supply			
2.4	IEEE 802.1D Spanning Tree Protocol, IEEE 802.1w Rapid Spanning Tree Protocol and IEEE 802.1s Multiple Spanning Tree Protocol			
2.5	IEEE 802.3ad Link Aggregation Control Protocol (LACP)			

20. Component: Access Switch 24 Port

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
3	Layer 2 Features			
3.1	Shall support up to 4,000 IEEE 802.1Q-based VLANs			
3.2	Shall support GARP VLAN Registration Protocol or equivalent feature to allow automatic learning and dynamic assignment of VLANs			
3.3	Shall have the capability to monitor link connectivity and shut down ports at both ends if uni-directional traffic is detected, preventing loops			
3.4	Shall support IEEE 802.1ad QinQ			
3.5	Shall support Jumbo frames on GbE ports			
3.6	Internet Group Management Protocol (IGMP)			
3.7	Multicast Listener Discovery (MLD) snooping			
3.8	IEEE 802.1AB Link Layer Discovery Protocol (LLDP)			
3.9	Shall support Voice VLAN feature to automatically assigns VLAN and priority to devices like IP phones			
4	Layer 3 Features (any additional licenses required shall be included)			
4.1	Static Routing for IPv4			
4.2	Static Routing for IPv6			
4.3	User Datagram Protocol (UDP) helper function to allow UDP broadcasts to			

20. Component: Access Switch 24 Port				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
	be directed across router interfaces			
4.4	Dynamic Host Configuration Protocol (DHCP) client and Relay			
4.5	Proxy ARP to allow normal ARP operation between subnets			
5	QoS and Security Features			
5.1	Access Control Lists for Layer 2 to Layer 4 traffic filtering			
5.2	Shall support global ACL, VLAN ACL, port ACL, and IPv6 ACL			
5.3	Traffic classification using multiple match criteria based on Layer 2, 3, and 4 information			
5.4	Powerful QoS feature supporting strict priority (SP) queuing, weighted round robin (WRR) / SP+WRR or equivalent			
5.5	Shall support applying QoS policies on a port, VLAN, or whole switch, to set priority level or rate limit selected traffic			
5.6	IEEE 802.1x to provide port-based user authentication with multiple 802.1x authentication sessions per port			
5.7	Media access control (MAC) authentication to provide simple authentication based on a user's MAC address			
5.8	Dynamic Host Configuration Protocol (DHCP) snooping to prevent unauthorized DHCP servers			

20. Component: Access Switch 24 Port				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
5.9	Port security and port isolation			
5.1	STP BPDU port protection to prevent forged BPDU attacks			
5.11	STP Root Guard to protect the root bridge from malicious attacks or configuration mistakes IP Source guard to prevent IP spoofing attacks			
5.12	IP Source guard to prevent IP spoofing attacks			
5.13	Dynamic ARP protection blocking ARP broadcasts from unauthorized hosts			
6	Management Features			
6.1	Configuration through the CLI, console, Telnet, SSH and Web Management			
6.2	SNMPv1, v2, and v3 and Remote monitoring (RMON) support			
6.3	sFlow (RFC 3176) or equivalent for traffic analysis			
6.4	Management security through multiple privilege levels			
6.5	FTP, TFTP, and SFTP/SCP support			
6.6	Port mirroring to mirror ingress/egress ACL-selected traffic from a switch port or VLAN to a local or remote switch port			
6.7	RADIUS/TACACS+ for switch security access administration			

20. Component: Access Switch 24 Port

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
6.8	Network Time Protocol (NTP) or equivalent support			
6.9	Shall have Ethernet OAM (IEEE 802.3ah) management capability			
7	Environmental Features			
7.1	Shall provide support for RoHS and WEEE regulations			
7.2	Shall have features to improve energy efficiency like variable-speed fans, shutoff unused ports etc			
7.3	Operating temperature of 0°C to 45°C			
7.4	Safety and Emission standards including UL 60950-1; IEC 60950-1; VCCI Class A; EN 55022 Class A			
8	Additional Requirement			
8.1	The switch should have Enterprise class of product			
8.2	System should be tested and certified for EAL 2 or above or NDPP certified			

21. Component: Access Switch 8 Port

Sr. No.	Description of Requirement	Compliance (Yes/No)	Details of Reference Document for verifying compliance	Reference Page No
1.	Switch Architecture			
1.1	The switch should have 8 X 10/100/1000 Base-Tx ports; all ports shall be 802.3af/at compliant PoE+ capable, with the switch support minimum			

21. Component: Access Switch 8 Port				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
	of PoE power budget as per 802.3at/af standard			
1.2	The switch should also support PoE as per 802.3af on all ports.			
1.3	Switch should have 8 Nos. 10 Base-T/100Base-Tx/1000Base-Tx auto-sensing ports complying to IEEE 802.3, IEEE 802.3at, IEEE 802.3u and 802.3ab standard, supporting half duplex mode, full duplex mode and auto-negotiation on each port.			
1.4	Switch should have minimum 2 dedicated SFP ports.			
1.5	The switching fabric for all the LAN ports shall be non-blocking and each port shall run at wire-speed / line-rate. Switching fabric capacity of the switch should be capable to run all the ports at line-rate.			
1.6	Switch should support both IPv4 and IPv6 – Switch should support features like Neighbor Discovery, Syslog, Telnet, SSH, Web GUI, SNMP, NTP, DNS, RADIUS overIPv6			
1.7	Switch should have non-blocking switching bandwidth of minimum 20Gbps			
1.8	Switch should have forwarding rate of minimum 14Mpps.			
1.9	Switch should be IPv6-Ready from Day 1			

21. Component: Access Switch 8 Port				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
2.	Layer 2 Features			
2.1	IEEE 802.1Q VLAN tagging			
2.2	802. 1Q VLAN on all ports with support for minimum 255 VLANs			
2.3	Support for minimum 8k MAC addresses			
2.4	Spanning Tree Protocol as per IEEE 802.1d.			
2.5	Multiple Spanning-Tree Protocol as per IEEE 802.1s.			
2.6	Rapid Spanning-Tree Protocol as per IEEE 802.1w.			
2.7	Self-learning of unicast & multicast MAC addresses per switch port.			
2.8	Jumbo frames up to 9000 bytes.			
2.9	Link Aggregation Control Protocol (LACP) as per IEEE 802.3ad.			
3	Security Features			
3.1	Switch should support MAC Address based Filters / Access Control Lists (ACLs) on all switch ports.			
	Switch should support Port based Filters / ACLs.			
3.2	Switch should support RADIUS and TACACS+ for access restriction and authentication.			
3.3	Secure Shell (SSH) Protocol, HTTP and DoS protection			
3.4	ARP spoofing, DHCP snooping etc.			
3.5	Switch should support static ARP, Proxy ARP, UDP forwarding and IP sourceguard.			
4	Management Features			

21. Component: Access Switch 8 Port

Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
4.1	The switch should support CLI as well as web-based Management.			
4.2	Switch should be SNMP manageable with support for SNMP Version 1, 2 and 3			
4.3	Switch should support all the standard MIBs (MIB-I & II).			
4.4	Switch should support TELNET and SSH Version-2 for Command Line Management			
4.5	Switch should support 4 groups of embedded RMON (history, statistics, alarm and			
	events).			
4.6	Switch should support System & Event logging functions as well as forwarding of these logs to multiple syslog servers.			
4.7	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.			
4.8	Switch should have comprehensive debugging features required for software & hardware fault diagnosis.			
4.9	Switch should support multiple privilege levels to provide different levels of access.			

21. Component: Access Switch 8 Port				
Sr. No.	**Description of Requirement**	**Compliance (Yes/No)**	**Details of Reference Document for verifying compliance**	**Reference Page No**
4.1	Switch should support NTP (Network Time Protocol).			
4.11	Switch should support FTP/TFTP for software upgrade			
4.12	Switch support multiple configuration file & backup configuration file.			
5	Additional Requirement			
5.1	The switch should have Enterprise class of product			
5.2	System should be tested and certified for EAL 2 or above or NDPP certified			

H. Annexure 3 – Indicative Bill of Material

Technical Specification for Central System in the Annexure 3 will be read as follows

Cloud DC DR Bill of material			
#	**Item**	**Min. Indicative**	**Min. Indicative Quantity of VMs at Disaster recovery Site**
		Quantity for VMs at Primary Data Center Site	
1	Web Server (Internal & External Traffic)	8	Functional DR with at least 50% compute capacity and 100% storage as that of Primary site.
2	Database Server	5	
3	Application Server	5	
4	API Services - Server	1	
5	Database Storage	5 TB	
6	Other Servers	As Required	
7	Server (min per server)	50 GB per Server	
8	Security Components	As Required	
9	Network Components	As Required	