REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION

000100/HO IT/RFP/734/2021-2022

UNITED INDIA INSURANCE CO. LTD

INFORMATION TECHNOLOGY DEPARTMENT
19,4th Lane
Uthamar Gandhi Salai
(Nungambakkam High Road)
Chennai – 600034
CIN : U93090TN1938GOI000108

Important Notice

This document is the property of United India Insurance Company Ltd (UIICL). It should not be copied, distributed or recorded on any medium (electronic or otherwise) without UIICL's written permission. Use of contents given in this document, even by the authorised personnel/agencies for any purpose other than that specified herein, is strictly prohibited and shall amount to copyright violation and thus, shall be punishable under the Indian Law. This tender document is not transferable.

Bidders are advised to study this tender document carefully. Submission of bid shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications.

The response to this tender should be full and complete in all respects. Incomplete or partial bids shall be rejected. The Bidder must quote for all the items asked for, in this tender.

The Bidder shall bear all costs associated with the preparation and submission of the bid, including cost of presentation and demonstration for the purposes of clarification of the bid, if so desired by UIICL. UIICL will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

Contents

PURPOSE OF THIS DOCUMENT

The purpose of this Request for Proposal (hereafter referred to as "RFP") is to define the scope of work for the Bidder for UIIC's Technology Refresh for DC and DR Infrastructure.
This RFP contains details regarding the scope, project timelines, evaluation process, terms and conditions as well as other relevant details which the Bidder needs to factor in while responding to this RFP.

DEFINITION OF TERMS USED IN THIS DOCUMENT

Company/UIIC/purchaser	United India Insurance Company Limited
EMD	Earnest Money Deposit
BG	Bank Guarantee
Vendor/Bidder	Is a company, which participates in the tender and submits its proposal
Products/equipment	Materials, which the Successful Bidder is required to SUPPLY, INSTALL, TEST, COMMISSION AND MAINTAIN as per this tender
Successful Bidder	A company, which, after the complete evaluation process, gets the Letter of Acceptance
Letter of Acceptance / LOA	A signed letter by the Purchaser stating its intention to award the work mentioning the total Contract Value
OEM	Original Equipment Manufacturer
SLA	Service Level Agreement
SP	Service Provider
SI	System Integrator
DC	Data Center
DR	Disaster Recovery
RCA	Root Cause Analysis
AMC	Annual Maintenance Contract
RFP	Request for Proposal
SOW	Scope of Work
T&C	Terms and Conditions
TCO	Total Cost of Ownership
EOS1	End of Sale
EOS2	End of Support
ATS	Annual Technical Support

SECTION 1 - BID SCHEDULE AND ADDRESS

S#	Description	Description
1.	Name of the Tender	REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION
2.	Tender Reference Number	000100/HO IT/RFP/734/2021-2022
3.	Tender Release Date	14-03-2022
4.	Last date for queries through email (rfp.email@uiic.co.in)	25-03-2022
5.	Pre-bid meeting	30-03-2022 (11.00 AM at our Head Office / Online)
6.	Last date for bid submission	07-04-2022 (03:00 PM)
7.	Address for submitting of Bids	The Deputy General Manager Information Technology Department Head Office, # 19, 4th Lane Uthamar Gandhi Salai, Nungambakkam High Road Chennai – 600034
8.	Tender Fee (Non-Refundable)	₹ 25,000 /- (Rupee Twenty-Five Thousand only)
8.	EMD Fee	₹ 25,00,000 /- (Rupees Twenty-Five lakhs only)
9.	Email ID for communication	rfp.email@uiic.co.in

Note:

1. Bids will be opened in the presence of the Bidders' representatives who choose to attend.
2. Any queries relating to the process of online bid submission or queries relating to e-Nvidia Portal, in general, may be directed to the 24x7 e-Nivida Helpdesk.
3. The contact number for the helpdesk is **Gagan (8448288987/89/eprochelpdesk.01@gmail.com), Ambika (8448288988/94/eprochelpdesk.02@gmail.com), Retnajith (9355030607), Sanjeet (8882495599), Rahul Singh (8448288982), Amit (9355030624), Abhishek Kumar (9355030617), Tariq (9355030608)**

SECTION 2 – INTRODUCTION

2.1 ABOUT UIIC

United India Insurance Company Limited (UIIC) is a leading public sector General Insurance Company transacting General Insurance business in India with Head Office at Chennai, 30 Regional Offices, 7 Large Corporate and Brokers Cells and 2000+ Operating Offices geographically spread throughout India and has over 13000+ employees. United India Insurance Company Limited, hereinafter called "UIIC" or "The Company", which term or expression unless excluded by or repugnant to the context or the meaning thereof, shall be deemed to include its successors and permitted assigns, issues this bid document, hereinafter called Request for Proposal or RFP.

2.2 OBJECTIVE OF THIS RFP

The purpose of this Request for Proposal (hereafter referred to as "RFP") is to define scope of work for the supply, installation and maintenance of hardware and supplied software at UIIC Datacentre, Mumbai & Disaster Recovery site, Hyderabad for UIIC Corporate Mailing Solution. Currently UIIC has 15,000 user based HCL Domino CCB licenses valid till 31-Aug-2022. Bidder has to factor ATS for the remaining contract period. This RFP contains details regarding scope, project timelines, evaluation process, terms and conditions as well as other relevant details which bidder needs to factor while responding to this RFP.

The System Integrator has to provide, manage and maintain all necessary infrastructure components & services that would be necessary as per the defined requirements of this RFP and subsequent addendums/corrigendum if any. The System Integrator has to ensure that the desired objective of UIIC's infrastructure is fulfilled.

2.3 DUE DILIGENCE

The Bidders are expected to examine all instructions, terms and specifications stated in this RFP. The Bid shall be deemed to have been submitted after careful study and examination of this RFP document. The Bid should be precise, complete and in the prescribed format as per the requirement of this RFP document. Failure to furnish all information or submission of a bid not responsive to this RFP will be at the Bidders' risk and may result in rejection of the bid. The decision of UIIC on rejection of bid shall be final.

2.4 ELIGIBILITY CRITERIA

S#	Eligibility Criteria for Bidders	Documentary Proof Required
1.	The Bidder should be a Registered Company in India under the 'Companies Act' and should be in existence in India for more than five (05) years as on 31.12.2021.	Copy of the Certificate of Incorporation issued by Registrar of Companies.
2.	The bidder should be authorized by the OEMs of the proposed equipment/devices and solution to bid for this tender.	MAF as per annexure 3 for Authorised partner. Self-declaration if the bidder is an OEM.
3.	The bidder should have an average annual financial turnover of at least ₹ 50 Crore for the last three financial year's viz. 2018-19, 2019-20, and 2020-21.	Audited financial statements / Certificate from Auditor
4.	The bidder should have made Net Profit after taxation in one of the last three financial years viz. 2018-19, 2019-20, and 2020-21.	Audited financial statements / Certificate from Auditor
5.	The bidder should not have been blacklisted/ debarred by any Government Departments, Agencies or Public Sector Undertakings in India as on the date of submission of the tender	As per annexure 2: No Blacklist declaration
6.	Bidder should have its own Support center for Telephonic and Remote Assistance Services in Chennai, Mumbai / Navi Mumbai & Hyderabad	Self-Declaration along with the details of the support centers in Chennai, Mumbai / Navi Mumbai & Hyderabad.
7.	As per the Government guidelines on Procurement bidder needs to submit the Annexure 14	Bidder needs to Submit Annexure 14 on letter head dully signed by Authorized signatory.
8.	Pre-Integrity Pact	Bidder needs to submit to copies of Pre-Integrity Pact as per Annexure 11.

SECTION 3 – SCOPE OF WORK

3.1 SCOPE OF WORK DUIRNG IMPLEMENTATION PHASE

UIIC currently has its Data Centre (DC) in Mumbai & Disaster Recovery Center (DR) in Hyderabad and HO in Chennai (UIIC reserves the right to shift its DC & DR to any part of India in future). The objective of this RFP is to size, supply, implement, maintain the entire solution as per scope outlined in this RFP. The Scope includes supply, installation, implementation, migration, integration, maintenance, and support of the solutions with all the relevant applications and infrastructure during the contract period.

Broad Scope of work will include but not be restricted to the following. Successful bidder will supply and install the solution as per the broad objectives as given below:

a. UIIC envisages refresh of its existing Infrastructure deployed at UIIC's DC, DR for corporate email solution.
b. Supply, installation, configuration & maintenance of all the supplied hardware and software at the DC & DR and seamless migration of entire data and integration with existing Network Architecture of UIIC.
c. All in-scope hardware & software should be provided with 3 years of comprehensive on-site warranty which will start from the date of GO-LIVE for all the solution hardware by UIIC and 2-year AMC. Bidder is required to co-ordinate with UIIC's existing System Integrator for migration activities and taking transition for Network activities.
d. The bidders shall quote AMC/ATS Charges for the solution for a period of 2 years after the initial comprehensive onsite warranty period of 3 years.
e. As the late sign-off of any solution may impact the Warranty / AMC timelines under back-to back agreements of SI with OEM, they are advised to take care of the same in their agreements with OEMs. UIIC will not consider any request for adjustments in such cases and will seek full five-year active life of each solution with full OEM support & services after acceptance and starting date of solution (GO-LIVE) in UIIC environment.
f. The comprehensive onsite warranty shall be with OEM back-to-back to support. The word "warranty" in this document refers to "comprehensive onsite warranty".
g. For All applications UIIC is looking for the x86 virtualized environment.
h. Bidder to factor the onsite manpower under FMS for a 24x7 support for the entire contract period. One resource to be placed at UIIC Head Office, Chennai. Resource as and when required at UIIC DC and DR sites should also be factored in the event of any contingency, at no additional cost to UIIC.
i. Bidder shall be responsible for closing of the VAPT and Audit findings, as and when UIIC communicates, within 15 days of communication of these findings, during the entire period of the contract.
j. The proposed solution at DR site should have same capacity and licensing as that of the DC.
k. Migrate complete data (approximately 75 TB) from existing storage (Domino e-mail data) to newly deployed hardware.
l. Migration includes migration of user data (email, calendar, contact data etc) and functional / configuration data (existing groups, mailing lists, relay configuration etc) as per UIIC requirements.
m. Bidder should integrate the solution with existing security solutions of UIIC's SOC-NOC project and other internal systems of UIIC. Integration needs to be carried out both at DC and DR.

n. All the patches/versions/upgrades/updates should be applied as and when released by the OEM in time bound manner.
o. For its DC and DR, UIIC envisages procurement and implementation of both LAN and SAN structured cabling.
p. Bidder to quote for all in-scope infra and application software and other in-scope components as part of the RFP. UIIC at its discretion shall procure application software where it has competitive arrangement with the OEM.
q. Bidder is required to provide details of each individual proposed infra, all software including management, performance monitoring tools and other in-scope components along with its associated hardware & software and any other component/service necessary for installation and implementation.
r. All necessary Power strips, Power cables, Network cables, Fiber cables and any other components required for successful implementation of the solution are to be supplied and commissioned by the successful bidder at no additional cost to the UIIC.
s. End of Support refers to the last day when the OEM will stop releasing the patches, security updates, bug fixing, and the components will not be available for replacement & product will be no longer supported by the OEM. Bidder should ensure that proposed hardware and software components should not go end of support within 7 years of date of delivery of the device/ and software, the same responsibility shall so survive even after termination or expiry of the contract. Bidder needs to give a declaration from the respective hardware OEM on their letterhead as per the Annexure -17 (Hardware End of Life and Support Declaration) of the RFP.
t. Bidder is required to supply, install, implement, commission, integrate and provide comprehensive on-site warranty/ATS of all the in-scope server hardware and software based on the Bill of Materials. The delivery plan must be synchronized with the project delivery timelines of UIIC.
u. Bidder is required to provide resources, which may be required for successful completion of the entire assignment within the quoted cost to UIIC.
v. Any coordination with the OEM for support should be carried out by the bidder only.
w. The warranty also includes all software subscriptions (critical hot fixes, service packs, and all upgrades/updates) of all components supplied as part of solution, wherever applicable.
x. The Hardware appliances proposed by the bidder should be rack mountable at DC and DR.
y. The successful bidder should submit the architecture design, detailed project plan, configuration, implementation plan along with the documentation on detailed solution architecture diagram. Presentations from the respective OEM should be done, if required.
z. The successful bidder has to deploy OEM certified engineers having expertise on proposed solutions at UIIC's Data center & DR site during the implementation process and ensure that the activity is to be carried out strictly in accordance with the OEM's design and the industry's best practices & guidelines.
aa. Provide 24x7 OEM support for the equipment and software components supplied as part of this tender.
bb. Provide updates, upgrades/new version for the software components during the warranty and maintenance period and installation of the same in co-ordination with UIIC team.
cc. All the equipment (hardware, software) supplied as part of solution should be IPV4 as well as IPV6 compliant from day one and should support all the protocols.
dd. During warranty period, UIIC may, shift the equipment to other location(s) within the Country. The bidder needs to ensure that the OEMs and bidders' warranty and support is valid across India. Further, bidder should undertake to continue to provide warranty and support for the supplied inventory at the new location at no additional cost to UIIC. Bidder will be informed

about old and new location details as and when UIIC decides to shift the hardware due to operational requirements. Bidder will deploy resource(s) for decommissioning of respective equipment at old location and Commissioning of equipment at new location at no additional cost. For such shifting, the charges towards packing, physical shifting and insurance would be borne by UIIC.

ee. The bidder should also provide support for un-mounting and mounting of hardware and other components supplied from the rack in the event of reallocation of racks or changes made at site based on company requirements.

ff. UIIC envisages to implement stretch cluster for the in-scope solution between DC and DR sites. Bidder must comply for the same and implement it for the company.

gg. Sign-off shall be given after successful commissioning of the solution, post installation and commissioning of appliance & software at all locations (DC and DR), all respective technical parameters should be implemented, complete data migration etc.

hh. Bidder should mandatorily plan drill activities quarterly once, between the DC and DR sites (or) whenever UIIC insists.

ii. Bidder to implement all HCL collaboration components which UIIC is entitled for in the proposed HCI infrastructure.

jj. Bidder should implement Bulk Mailing solution as per the technical specification and bidder should assist UIIC or initiate the bulk emails as and when required with the solution deployed.

kk. Under no circumstances UIIC IP address should be used for bulk mailing purpose.

ll. Bidder should implement Verified mark certificate (VMC) for all UIIC outbound emails which should have the verified logo as per the security standards.

Bidder is, also, required to carry out activities given in the following table:

S#	Activity	Remarks
1	Physical delivery of all hardware; its related software, software licenses, hardware for archiver appliance, backup appliance, mailing solution and MDM Solution.	Bidder has to supply and deliver server hardware; its related software, software licenses, hardware and software for archiver appliance, backup appliance, mailing solution, MDM Solution and other components and cables for DC and DR site. All Hardware stack delivered as part of the RFP should be compatible with each other.
2	End-to-end installation and implementation of server hardware; its related software, software licenses, hardware and software for archiver appliance, backup appliance, Mailing solution, MDM Solution and Structured Cabling components, at DC and DR.	Bidder/OEM is required to do end-to-end installation, implementation and configuration of in-scope server hardware and/or application software. Bidder/OEM is required to unpack, assemble, mount and boot the equipment, install necessary service packs, patches and fixes, set up and configure the equipment. Compatibility issues of sub-systems with OS, respective drivers, firmware, any other components are to be installed, if required, are to be resolved by bidder/OEM. Post end-to-end installation and implementation of equipment by bidder, UIIC will conduct acceptance test to verify installation's compliance with the configuration and relevant setting provided by UIIC.

3	Provide comprehensive on-site warranty and ATS support for the tenure of contract period.	Bidder will be responsible to provide comprehensive on-site warranty and back-to-back support from the OEM to meet the Service Levels defined in this RFP till Validity of the Contract. Warranty of hardware will start from the GO-LIVE as mentioned and ATS shall start from the GO-LIVE date except for HCL Domino which will be as per the respective expiry date mentioned earlier.
4	Implementation and Assessment Services	Bidder will be responsible to provide implementation and assessment services as per the scope defined in this RFP. OEM along with the bidder shall do the implementation and assessment of in-scope components, however, for UIIC, bidder would be the single point of contact for Implementation and Assessment services.
5	Migration Services	Bidder/OEM will be responsible to provide migration services as per the scope defined in this RFP.
6	Integration with UIIC NOC & SOC	Bidder shall be responsible for integration the solution stack with UIIC Noc & Soc.
7	License Details	All licenses shall be procured in the name of UIIC. Complete license certificate/document should be submitted as physical/soft form to UIIC.

3.1.1 X86 Servers at DC and DR

UIIC existing email infrastructure comprises IBM Power 710 servers (214FDFV, 214FDCV, 214FDDV) at DC & DR. UIIC envisages refresh of existing IBM Power servers with hyper converge infrastructure. Refer to Annexure 9 – Minimum Functional & Technical Specification for hardware & software details and compliance requirements for hyper converge. Bidder is required to supply, install, implement, commission, integrate and provide comprehensive onsite warranty, FMS & ATS – during the period of contract, for the proposed hyper converge and associated software to be hosted at DC & DR. In addition, Bidder is required to supply, install, commission and provide onsite warranty, FMS & ATS during the period of contract for the racks mentioned in Annexure 9 – Minimum Functional & Technical Specification.

Successful bidder will configure inbuilt storage of Hyper-Converged Infrastructure/inbuilt Network/Compute with High Availability and Optimize resources by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g. Storage, processing, bandwidth and active user accounts) to obtain optimum performance level. The resource usage should be monitored, controlled and reported to HCI admin through single central management console.

The bidder should make sure that the solution should support defined Recovery Time Objective when the VMs are moved from DC to DR.

3.1.2 HIPS for Virtualized x86 environment

The bidder needs to supply, install, size, configure, maintain the HIPS tool for proposed Hyper converge infrastructure. The bidder needs to factor all the License, installation, commission, integration cost in the Annexure 7 Commercial Bid Format. The proposed tool should follow the technical specification mentioned in the Annexure 9 – Minimum Functional & Technical Specifications.

The proposed tool should be integrated with the existing SIEM (McAfee) of the UIIC, and the bidder needs to provide a report as per the agreed frequency to UIIC stakeholders showcasing the patch details and other malware attack and protection done by the tool.

3.1.3 Backup Solution at DC and DR

Bidder needs to propose backup solution to follow the technical specification mentioned in the Annexure 9-Minimum functional & technical specifications. The backup solution will be used for the doing backup of the DB, Operating system & Application etc. All required licenses also to be factored as part of the solution with the necessary ATS.

3.1.4 Storage & Switch

For the Storage and San switches mentioned in UIIC has provided the minimum functional & technical specification in Annexure 9. Bidders need to ensure that the solutions proposed comply with these minimum technical requirements.

Vendor will have to complete the successful migration of data from old storage to new external storage. Migration of data to be ensured with minimum near zero downtime. Vendor must have sufficient skill sets required for virtualising existing storages for performing the seamless data migration with no data loss. Skill sets should include expertise in SAN Network, SAN Storage and connected servers.

3.1.5 Phase wise activities

Bidder will complete the required activities in the following manner

Kick-Off Meeting	Vendor will: •Conduct a Kick-off Meeting with the UIIC stakeholders to review the project Scope, Approach, Deliverables and responsibilities of both parties. •During the Kick-off Meeting, Vendor will exchange contacts, procedural and schedule information with UIIC.
Pre-site Tasks	• At least one week prior to commencing Service at the Service Location, Vendor will provide UIIC with a Pre-site Readiness Checklist. Vendor will verify that the necessary prerequisites listed in the Pre-site Readiness Checklist have been completed. Checklist includes an inventory of UIIC's environment included in the Scope of the Service. • Vendor will meet with the UIIC to confirm logistics, such as user access and workspace, and identify any modifications to UIIC's inventory in the Pre-site Readiness Checklist. • When the Pre-site Readiness Checklist is completed and verified by Vendor, Vendor and UIIC will schedule the Service to commence at the Service Location.
Discovery	Vendor will: • Collect host path level information, if any, including: o Host (physical and virtual), HBA, SAN (fabric, firmware, names), details and mapping o Legacy storage hardware, port, LUN information and details o Storage allocations and usage • Data will be collected and analysed. • All data gathered in the Discovery Phase will be validated for its accuracy and relevance to the data path analysis. The data will then be compared against Vendor Product Support and Software Matrix to validate its supported levels of OS and firmware, etc. and documented. o Interim Support Requests will be created as necessary o Suggestions for driver, firmware, and/or hardware updates will be made
Plan and Design	Vendor will: • Conduct interviews with UIIC as required to validate the technical details gathered earlier as needed to perform the Service. • Work with UIIC to design and plan the required Migration Tasks. • Document the software configuration storage management tool in the migration Plan. • Create a project plan and migration plan. • Compare the overall project schedule and number of migration events and their duration with the Migration Schedule per week, including: o Mapping of source to target environment o Schedule pre-planning work and group hosts within UIIC provided outage and maintenance windows o Review final migration steps and schedule outage meetings o Validate UIIC Change request, conduct walk-through of tasks and events

Testing and Validation	Vendor will: • Assist UIIC with the verification of the data migration and of the accessibility of that data by UIIC's team. • Once UIIC and Vendor have agreed that the designated LUN for an identified migration event has been migrated, designated host servers are running using new storage, and that UIIC's applications have resumed processing, UIIC's project team will validate the completed event including data level validation. The vendor should certify and ensure zero data loss and successful migration of data to new storage.
Knowledge Transfer	Vendor will: · Provide Knowledge Transfer to UIIC's technical staff throughout the delivery of Service, which includes a detailed overview on the implementation and configuration parameters and features and functionality of the new storage system(s).
Project Closure	Vendor will: • Review the target storage system(s) and host server environment with the migrated data with UIIC's project team. • Review Service-related documents with UIIC. • Review troubleshooting, support, and escalation procedures with UIIC.

Vendor is required to designate a project coordinator who is responsible for the overall project and coordination of project management activities with UIIC's Project Manager. The project coordinator will have responsibility for coordinating all activities on this engagement, scheduling resources, and will be the single point of contact for Vendor for this Service.

3.1.6 Buy Back

UIIC expects to protect the investment already made on the existing components thus the Bidder is also required to buyback the specified inventory as mentioned in RFP. Buy back items are available at DC and DR. However, buy back is subject to UIIC's discretion. If any item is required for future use, UIIC may remove it from buy-back offer. Bidder must collect item in as-is-where-is condition. No additional expenses will be paid for removal of items. Destruction of hard disks and magnetic tapes should be done in the presence of UIIC representative. The commercials quoted by the Bidder should include the buyback price assessed by the Bidder. The Purchase price once accepted by the UIIC cannot be withdrawn.

It should be the bidder's responsibility to collect the buyback items, from UIIC's location and UIIC will not provide any transportation expenses towards this. It would be the bidder's responsibility to ensure safe disposal of e-waste as per Hazardous Waste (management and handling) Rules 1989 and 2008, without imposing any liability to UIIC, comprising discarded Hardware/ electrical/ electronic equipment/components taken under buyback.

3.2 SCOPE OF WORK FOR FACILITY MANAGEMENT PHASE

The facility management will commence once the end-to-end solution is implemented, tested and accepted by the company. The bidder should include the cost for implementation, testing and acceptance procedure in the implementation charges and no additional charges will be paid during this period.

Complaint(s) can be booked by onsite engineers or HO officials. Breakdown/ failure calls will be intimated to the bidder by Telephone/ Web/ Fax / E-mail etc. The bidder should compulsorily allot a complaint ID for every complaint booked by any office by any medium. The downtime / breakdown period will be reckoned from the date and time of logging of the complaint by UIIC.

Bidder must factor a web-based ticketing tool as part of the solution.

The bidder shall guarantee an **uptime of 99%** for the equipment supplied at DC and DR, during Warranty period, which **shall be calculated on monthly basis.**

The "Downtime" is the time between the Time of Report by the company and Time of Restoration/resolution within the contracted hours. "Failure" is the condition that renders the company unable to access the services hosted in DC / DR site. "Restoration" is the condition when the selected bidder demonstrates that the services hosted in DC and DR site are accessible.

The Downtime calculated shall not include any:

a) Failure due to company (Power, cabling fault, servers etc.)
b) Preventive maintenance activity and
c) Force Majeure.

The percentage uptime is calculated on monthly basis (24 hours a day).

The performance would be measured as under on monthly basis:

$$\text{Performance (\%)} = \frac{\text{(Total contracted minutes in a month – downtime Minutes within contracted minutes in a month)}}{\text{Total contracted minutes in a month}} \times 100$$

Shortfall in performance = uptime % - Performance %

Severity Levels of Incidents

Severity Level	Criteria	Indicative list of issues
Severity 1	The identified issue has material business impact and needs to be resolved immediately. This level would typically correspond to issues that result into disruption of most or all critical services to UIIC.	• Issues pertaining to application and related databases, system software, hardware which make the application inaccessible. • >10% of users are affected.
Severity 2	The identified issue has significant business impact and needs to be taken up on top priority.	• User management or helpdesk infrastructure not functioning properly.

		• A temporary workaround is available. • Impaired operations of some components, but allows the user to continue using the software
	This level would typically correspond to issues that result into disruption of one or more critical services to UIIC	
Severity 3	The identified issue has normal impact on the business and needs to be addressed at the earliest.	• User requests like password reset, signature updations, etc. • Licensing issues, software issues which are not business critical. • Includes "how to" questions and issues impacting individual users.
	This level would typically correspond to issues which result into disruption of one or more services to one or more USERS.	
Severity 4	The identified issues have almost no impact in terms of business.	• Additional customization requirements. • Upgrade, major change, and migration notifications • Mobile configuration help
	However, issue needs the attention of the Bidder/System Integrator and shall be fixed on lesser priority.	

Penalties

Level	Reporting Time	Resolution Time	Penalty beyond stipulated resolution time
Severity 1	Business hours	1 hour	Rs.10000/= per hour of delay beyond the stipulated resolution time.
	Non-business hours	Start of business hours next day	0.25% of contract value plus Rs.10000/= per hour of delay beyond the stipulated resolution time.
Severity 2	Business hours	4 hours	Rs.5000/= per hour of delay beyond the stipulated resolution time.
	Non-business hours	Start of business hours next day	0.25% of contract value plus Rs.5000/= per hour of delay beyond the stipulated resolution time.
Severity 3	Business hours	4 hours	Rs.2500/= per hour of delay beyond the stipulated resolution time.
	Non-business hours	Start of business hours next day	0.25% of contract value plus Rs.2500/= per day of delay beyond the stipulated resolution time.
Severity 4	All hours	Start of business hours next day	Rs.100/= per day per call of delay beyond the stipulated resolution time.

BULK EMAIL PENALTY

For Time-bound Emails (for e.g. - Transactional Emails / OTP Emails / Email Alerts / Critical Application Alerts / etc.)

Sl. No.	Delay duration (Above Permitted time to deliver email*)	Penalty
1	Up to 1 minute	1 % of the bill for bulk emails for the Quarter
2	Up to 3 minutes	3 % of the bill for bulk emails for the Quarter
3	Over 3 minutes	5 % of the bill for bulk emails for the Quarter

**** Permitted time for delivery – 1 minute***

For Promotional / Campaign Emails / Informational Emails

Sl. No.	Delay duration (Above Permitted time to deliver email #)	Penalty
1	0-1000	1 % of the bill for bulk emails for the Quarter
2	1001-10000	3 % of the bill for bulk emails for the Quarter
3	10001 and above	5 % of the bill for bulk emails for the Quarter

 # Permitted time for delivery – 1 Hour

- The penalty shall be adjusted as maintenance credit against the AMC/ATS payable by UIIC to the Bidder/System Integrator.
- Record of call resolution is to be jointly signed by system integrator and UIIC personnel marking nature of fault attended and steps / initiatives taken to resolve the service call of the company.
- This service is to be provided on all working days of UIIC, notwithstanding the fact whether on such days the Bidder's office remains open or not. The Bidder's local representative and our Department Head will undertake the review of maintenance every month with monthly reports.
- The bidder must provide a web-based call logging system (ticketing tool) with provision to categorize the calls based on the severity. Monthly reports should be submitted for review of call resolution.
- The penalty amount will be calculated as per the Uptime/Availability mentioned in the Service Levels to an overall cap in a year of 2% of the Total Contract Value.

Minimum Qualification of onsite support engineers

- Graduate in science/Engineering with at least 2 years of experience in implementing and maintaining of on-premise HCL Domino mailing solution and infrastructure.
- Should have good knowledge on implementation, integration, troubleshooting and various functionalities of the proposed mailing solution along with the network aspects.
- Support personnel should be under bidders own payroll.
- Support personnel should be placed at UIIC Head Office premises / DC / DR locations as per UIIC choice during UIIC office hours. However, the hours may be extended whenever required.
- If the performance is not up to the mark, the personnel may have to be changed, if UIIC so requests.

RTO / RPO Management

The bidder needs to maintain the 120 minutes RTO and 0 (zero) minutes RPO parameters of the all the in-scope equipment's and software.

3.3 SINGLE POINT OF CONTACT

The selected Bidder shall appoint a single point of contact, with whom UIIC will deal with, for any activity pertaining to the requirements of this RFP.

SECTION 4 – INSTRUCTION TO BIDDERS

4.1 INSTRUCTIONS/GUIDELINES TO BIDDERS

- UNITED INDIA INSURANCE Co. Ltd. invites bids for the REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION
- Tender Bidding Methodology: 'Single Stage Online submission & Three stage online opening' [Prequalification, Technical Bid & Commercial Bid].
- The bidding process is completely online. Bidders are requested to submit all documents online as detailed in this RFP. Bidders should submit hard copy if demanded or a clarification is sought in this regard.

ONLINE SUBMISSION

- The bidders can access the documents in the UIIC e-tendering portal https://uiic.enivida.com
- Bidders can avail the service of the e-tendering service provider for registering themselves, accessing tender documents, and completing the tender submission formalities. The service provider will provide all necessary assistance to bidders for online bidding.
- For further instructions regarding submission of bids online, the bidders shall visit the e-tender portal (https://uiic.enivida.com).
- The relevant tender documents can be purchased/downloaded from the e-tendering site with the bidders authorized user credentials.
- The bidders should mandatorily fill in all relevant details as per the requested form in the e-tendering portal in all three sections i.e., Prequalification, Technical Bid & Commercial Bid and all relevant scanned copies to be attached.

1.1.1 ONLINE DOCUMENTS TO BE SUBMITTED

The bidders should mandatorily attach below scanned copies of the following documents in the respective sections.

- **PREQUALIFICATION DOCUMENTS (ONLINE SUBMISSION - SCANNED DOCUMENTS)**

  - RFP Document Fee submission proof.
  - Authorized signatory of the Bidder signing the Bid Documents should be empowered to do so as per Annexure 1. Proof in the form of letter signed by a director or Company Secretary to be attached.
  - No Blacklisting Declaration as per Annexure 2.
  - Letter of Authorisation / Manufacturer Authorisation by Power of Attorney of OEM as per Annexure 3.
  - Statement of Nil Deviations as per Annexure 4.
  - Proof of Earnest Money Deposit (EMD) amount deposited in UIIC Account / Bank Guarantee for EMD as per Annexure 5.
  - Eligibility Criteria Declaration Form as per Annexure 6. All supporting documents as detailed in Annexure 6.
  - Non-disclosure agreement to be submitted as per Annexure 8.
  - Bid Submission Check List as per Annexure.
  - Copy of this RFP duly signed and stamped / digitally signed as token of acceptance of all the terms and conditions of this tender.
  - Pre-Integrity Pact as per Annexure 11.
  - Annexure 15 from Bidder as well as all Proposed OEM's.

- **TECHNICAL BID DOCUMENTS (ONLINE SUBMISSION)**

  - Compliance Statement for the prescribed Technical specifications as per Annexure 9. Along with all supporting documents as detailed in Annexure 9.

- **FINANCIAL DOCUMENTS (ONLINE SUBMISSION)**

  - Commercial Bid to be submitted as per Annexure 7.

1.1.2 TENDER FEE

A non-refundable tender document fee of ₹ 25,000/- (Rupees Twenty-Five Thousand Only) shall be remitted through NEFT at least two days prior to the tender submission date to the below account

Beneficiary Name	**United India Insurance Company Ltd.**
IFSC Code	INDB0000007
Account No	200999095210000100ITEMAILTender
Bank Details	Indusind Bank
Remarks	TENDER_FEE_EMAIL<Depositor Name>

- The vendor shall provide commercial bid as per the format given in Annexure 7.
- EMD of Rs. 25,000/- (Rupees Twenty-Five Thousand only) in the form of Bank Guarantee / NEFT favouring UIIC shall be valid for six months.

- In case of EMD in the form of Bank Guarantee, the bidders shall adhere to the format enclosed along with this RFP. (REF. Annexure 5: Bank Guarantee Format)/Electronic Credit for EMD of Rs. 25,000/- (Rupees Twenty-Five Thousand only).
- Bank Guarantee shall be drawn in favour of "United India Insurance Company Limited" payable at Chennai.

1.1.3 PRE-BID MEETING

- Pre-bid meeting would be held as per the date specified in the Section 1 - Bid Schedule and Address.
- Intending bidders who wish to participate in the Pre-bid meeting shall submit the proof of payment of non-refundable Tender fee of Rs. 25,000/- only (Rupees Twenty-Five thousand Only) prior to the Pre-Bid meeting date.
- Documentary proof of payment of tender fee is a pre-requisite for attending the pre-bid meeting.
- Only authorized representative of Bidders (not exceeding two) would be allowed to participate in the pre-bid meeting.
- A copy of the proof of payment of non-refundable tender fee must be emailed to the following email id - 'rfp.email@uiic.co.in.
- Pre-bid queries should be mailed to us in the email id 'rfp.email@uiic.co.in' in the attached format in Annexure 12- Pre bid query format.
- Queries received after the due date as mentioned in Section-1 will not be entertained.
- Replies to the pre-bid queries would be posted on our website / e-nivida portal ONLY.

4.2 EARNEST MONEY DEPOSIT (E.M.D)

- The intending bidders shall submit Bank Guarantee (REF. Annexure 5: Bank Guarantee Format for EMD)/Electronic Credit for EMD of Rs. 25,00,000/- (Rupees Twenty-Five lakhs only). Bid will be treated as non-responsive and will be rejected in the absence of any one of the above mentioned.
- Bank Guarantee shall be drawn in favor of "United India Insurance Company Limited" payable at Chennai. The BG submitted as EMD should have a validity of 6 months.
- In case of Electronic Credit, the E.M.D shall be credited to our Bank Account as given below:

Beneficiary Name	**United India Insurance Company Ltd.**
IFSC Code	INDB0000007
Account No	200999095210000100ITEMAILTender
Bank Details	Indusind Bank
Remarks	EMD_FEE_EMAIL<Depositor Name>

- The EMD will not carry any interest.
- The electronic credit should be affected positively at least two days prior to the tender submission date.
- A non-refundable tender document fee of ₹ 25,000/- (Rupees Twenty-Five Thousand Only) shall be remitted through NEFT at least two days prior to the tender submission date to the below account:
- The above account details shall be used for remitting the non-refundable tender document fee as well.

4.3 FORFEITURE OF EMD

The EMD made by the bidder will be forfeited if:

- The bidder withdraws the tender after acceptance.
- The bidder withdraws the tender before the expiry of the validity period of the tender.
- The bidder violates any of the provisions of the terms and conditions of this tender specification.
- The successful bidder fails to furnish the required Performance Security within 15 days from the date of receipt of LOA (Letter of Acceptance)

4.4 REFUND OF EMD

- EMD will be refunded to the successful bidder, only after submission of PBG and signing of contract as per timelines defined in the RFP
- In case of unsuccessful bidders, the EMD will be refunded to them at the earliest after expiry of the final bid validity and latest on or before the 30th day after the award of the contract.

4.5 THE COMPANY RESERVES THE RIGHT TO

- Accept / Reject any of the Tenders.
- Revise the quantities at the time of placing the order.
- Add, Modify, Relax or waive any of the conditions stipulated in the tender specification wherever deemed necessary.
- Reject any or all the tenders without assigning any reason thereof.
- Seek clarifications from the prospective bidders for the purpose of finalizing the tender.

4.6 REJECTION OF TENDERS

The tender is liable to be rejected inter-alia:

- If it is not in conformity with the instructions mentioned herein,
- If it is not accompanied by the requisite proof of tender document fee paid.
- If it is not accompanied by the requisite proof of EMD paid.
- If it is not properly signed by the bidder.
- If it is received after the expiry of the due date and time.
- If it is evasive or incomplete including non-furnishing the required documents.
- If it is quoted for period less than the validity of tender.
- If it is received from any blacklisted bidder or whose experience is not satisfactory.

4.7 VALIDITY OF TENDERS

Tenders should be valid for acceptance for a period of at least 180 (One hundred and eighty only) days from the last date of tender submission. Offers with lesser validity period would be rejected.

4.8 GENERAL TERMS

- The successful bidder shall sign the agreement within 15 days from the date of Letter of Acceptance (LOA) from UIIC.
- The agreement shall be in force for a period of 5 (FIVE) years from the date of issue of Purchase Order and may be extended on mutually agreed terms.
- The offer containing erasures or alterations will not be considered. There shall be no handwritten material, corrections or alterations in the offer.
- Addendum/Amendments/Corrigendum, if any, will be communicated through UIIC e-Tendering portal (https://uiic.enivida.com/) only. UIIC reserves the right to cancel the tender at any time without incurring any penalty or financial obligation to any bidder.
- UIIC reserves its right to carry out inspection of the proposed solution facility, if required. There shall not be any additional charges for such inspection.
- UIIC is governed by provisions of the Public Procurement Policy for Micro and Small Enterprises (MSEs) as circulated by The Ministry of MSME, GoI. The policy details are available on the website www.dcmsme.gov.in
- These provisions shall be applicable to Micro and Small Enterprises (MSEs) registered with District Industries Centres or Khadi and Village Industries Commission or Khadi and Village Industries Board or Coir Board or National Small Industries Corporation or Directorate of Handicrafts and Handloom or any other body specified by Ministry of Micro, Small and Medium Enterprises (MSMEs).
- Such MSEs would be entitled for exemption from furnishing tender fee and earnest money deposit (EMD). In case of any issue on the subject matter, the MSE's may approach the tender inviting authority to resolve their grievances.
- Agencies/ Bidders desirous of availing exemptions/ preference under above provisions should submit a copy of proof of Registration as MSEs/ and ownership of the same by SC/ST along with the tender/RFP.
- The bidder to note that splitting of order would not be applicable in this tender.

4.9 SECURITY DEPOSIT

The successful bidder will have to furnish a security deposit of 3% on the total contract value in the form of a Bank Guarantee for a period of 5 years & 3 months obtained from a nationalized/ scheduled bank for proper fulfilment of the contract.

5 PRICE

- The bidders should quote only the base price. All applicable taxes will be paid as actuals.
- The price shall be all inclusive of labour cost, packing, forwarding, freight, transit insurance, Excise duty, road permit charges, other duties, if any, including state levy, delivery, installation, commissioning and testing charges.
- There shall be no escalation in the prices once the prices are fixed and agreed to by the Company and the bidders. But any benefit arising out of any subsequent reduction in the prices due to reduction in duty during the period between the date of Letter of Acceptance and the date of Purchase Order, should be passed on to the Purchaser /Company.

- All the items should be quoted in INR (Indian Rupees) only.

6 EVALUATION OF OFFERS

Each bidder acknowledges and accepts that the UIIC, in consultation with its appointed consultants, may in its absolute discretion apply selection criteria for evaluation of proposals for short listing / selecting the eligible bidders(s). The RFP document along with addendum/corrigendum if any, will form part of agreement to be signed / executed with the UIIC by the successful bidder through this procurement / evaluation process.

7 INSURANCE

The Bidder is responsible for acquiring transit insurance for all components. The goods to be transported under this Contract shall be fully insured in Indian Rupees.

8 NO COMMITMENT TO ACCEPT LOWEST OR ANY OFFER

- UIIC is under no obligation to accept the lowest or any other offer received in response to this tender and reserves the right to reject any or all the offers including incomplete offers without assigning any reason whatsoever.
- UIIC reserves the right to make any changes in the terms and conditions of the tender. UIIC will not be obliged to meet and have discussions with any Bidder or to entertain any representations.

9 FORMAT AND SIGNING OF BID

- Proposals submitted in response to this tender must be signed by (in all the pages) the Authorized signatory of the Bidder's organization as mentioned in the Power of Attorney or Letter of Authorization.
- The bid shall be in A4 size papers, numbered with index, highlighted with technical specification details, shall be signed by the Bidder or a person duly authorized to bind the Bidder to the Contract and neatly bind or filed accordingly.
- Any interlineations, erasures or overwriting may be considered invalid.
- Bids should be spirally bound or fastened securely before submission. Bids submitted in loose sheets may be rejected as non-compliant.
- Bidders responding to this tender must comply with the format requirements given in various annexure of the tender, bids submitted in any other format/type will be treated as non-compliant and may be rejected.
- ADDITIONAL INFORMATION: Include additional information which will be essential for better understanding of the proposal. This might include diagrams, excerpts from manuals, or other explanatory documentation, which would clarify and/or substantiate the bid. Any material included here should be specifically referenced elsewhere in the bid.
- GLOSSARY: Provide a glossary of all abbreviations, acronyms, and technical terms used to describe the services or products proposed. This glossary should be provided even if these terms are described or defined at their first use in the bid response.

10 PUBLICITY

Any publicity by the vendor in which the name of the Company is to be mentioned should be carried out only with the prior and specific written approval from the Company. In case the vendor desires to show any of the equipment to his customers, prior approval of the Company will have to be obtained by the vendor in writing.

11 ROYALTIES AND PATENTS

Any royalties or patents or the charges for the use or infringement thereof that may be involved in the contract shall be included in the price. Bidder shall protect the Company against any claims thereof.

12 PURCHASER'S RIGHT TO VARY QUANTITIES / REPEAT ORDER

The purchaser reserves the right at the time of award of the contract to increase the quantity of the goods and services specified in the schedule of requirements not exceeding 25% of the quoted quantities without any changes in unit price of the order quantity.

The purchaser reserves the right to place order for additional items of bill of material, apart from the numbers / locations mentioned in this RFP (OR) purchaser reserves the right to place order for additional items not exceeding 25% of the quoted quantities at the same rates and terms & conditions during a period of SIX MONTHS from the date of acceptance of Purchase Order by the bidder. No additional cost whatsoever other than the cost contracted would be paid. In case of any change in tax rates, the taxes prevailing at the time of placing repeat order would be applicable.

13 CHANGE / MODIFICATION IN LOCATIONS FOR DELIVERY/INSTALLATION/SUPPORT

Company reserves the right to change/modify locations for support of the items. In the event of any change/modification in the locations where the hardware items are to be delivered, the bidder in such cases shall deliver, install and support at the modified locations at no extra cost to UIIC.

In case the hardware items are already delivered, and if the modifications in the locations are made after delivery, the bidder shall carry out installation, testing and commissioning at the modified locations. UIIC in such cases shall bear the shifting charges/arrange shifting and the bidder shall shift the material to the alternate locations at mutually agreed prices if the Company so requests.
The Warranty should be applicable to the altered locations also.

14 LATE BIDS

Bidders are advised in their own interest to ensure that bid reaches the specified office well before the closing date and time of the bid. Any bid received after the deadline for submission of the bid, will be rejected.

15 INSPECTION AND TESTS

The Purchaser or its representatives or ultimate client shall have the right to inspect and test the goods for their conformity to the specifications. The Purchaser may also appoint an agency for this purpose. The technical specifications shall specify what inspection and tests the Purchaser requires and where they are to be conducted. Where the Purchaser decides to conduct such tests on the premises of the Supplier, all reasonable facilities and assistance like testing instruments and other test gadgets including access to the drawings and production data shall be furnished to the UIIC officials free of costs. In case the tested goods fail to conform to the specifications, the company may reject them, and the Supplier shall either replace the rejected goods or make alteration necessary to meet the specifications requirements free of cost to the Purchaser.

Notwithstanding the pre-supply tests and inspections, the material on receipt in the Purchaser's premises shall also be tested and if any material or part thereof is found defective, the same shall be replaced free of cost to the Purchaser.

If any material before it is taken over is found defective or fails to fulfil the requirements of the contract, the company shall give the Supplier notice setting forth details of such defects or failures and the Supplier shall make the material good or alter the same to make it to comply with the requirements of the contract and in any case within a period not exceeding 2 months of the initial report. These replacements shall be made by the Supplier, free of the all charges, at the site(s).

16 INDEMNIFICATION

The Bidder shall, at its own expense, defend and indemnify UIIC against any third party claims in respect of any damages or compensation payable in consequences of any accident or injury sustained or suffered by its (Bidder's) employees or agents, or by any other third party resulting from or by any gross negligence and/or wilful default by or on behalf of the Bidder and against any and all claims by employees, workmen, contractors, sub- contractors, suppliers, agent(s), employed, engaged, or otherwise working for the Bidder, in respect of any and all claims under the Labour Laws including wages, salaries, remuneration, compensation or like.

The Bidder shall indemnify, protect and save UIIC and hold UIIC harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly from a gross negligence and/or wilful default of the Bidder, its employees, its agents, or employees of the consortium in the performance of the services provided by this contract, breach of any of the terms of this tender document or breach of any representation or warranty by the Bidder, use of the deliverables and or services provided by the Bidder, Infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project.

The Bidder shall further indemnify UIIC against any proven loss or damage to UIIC's premises or property, etc., due to the gross negligence and/or wilful default of the Bidder's employees or representatives to the extent it can be clearly established that such employees or representatives acted under the express direction of the Bidder.

The Bidder shall further indemnify UIIC against any proven loss or damage arising out of loss of data, claims of infringement of third-party copyright, patents, or other intellectual property, and third-party claims on UIIC for malfunctioning of the equipment at all points of time, provided however:

UIIC notifies the Bidder in writing in a reasonable time frame on being aware of such claim, the Bidder has sole control of defence and all related settlement negotiations. UIIC provides the Bidder with the assistance, information and authority reasonably necessary to perform the above, and UIIC does not make any statement or comments or representations about the claim without prior written consent of the Bidder, except under due process of law or order of the court. It is clarified that the Bidder shall in no event enter into a settlement, compromise or make any statement (including failure to take appropriate steps) that may be detrimental to UIIC's (and/or its customers, users and service providers) rights, interest and reputation.

17 LIQUIDATED DAMAGES DURING DELIVERY, INSTALLATION & WARRANTY

The liquidated damage is an estimate of the loss or damage that UIIC may have suffered due to non-performance of any of the obligations (under the terms and conditions) or delay in performance during the contract relating to activities agreed to be undertaken by the Bidder.

If the bidder fails to deliver and install the Solution or to perform the services within the time period(s) specified in the contract, UIIC shall without prejudice to its other remedies under the contract, deduct from the contract price, as liquidated damages, a sum equivalent to the 1% of the contract price for every week (seven days) or part thereof of delay, up to maximum deduction of 10% of the contract price . Once the maximum is reached, UIIC may consider termination of the contract.

Liquidated damages are not applicable for reasons attributable to UIIC and Force Majeure. However, it is the responsibility/onus of the Bidder to prove that the delay is attributed to UIIC and Force Majeure. The Bidder shall submit the proof authenticated by the Bidder and UIIC's official that the delay is attributed to UIIC and Force Majeure along with the bills requesting payment.

Liquidated damages are applicable over and above all the penalties mentioned in RFP.

18 LIMITATION OF LIABILITY

Bidder's cumulative liability for its obligations under the contract shall not exceed 100% of Contract value and the bidder shall not be liable for incidental / consequential or indirect damages including loss of profit or saving.

19 INSOLVENCY

The Company may terminate the contract by giving written notice to the vendor without compensation, if the vendor becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to the company.

20 FORCE MAJEURE

The parties shall not be liable for default or non-performance of the obligations under the contract if such default or non-performance of the obligations under this contract is caused by Force Majeure.
For this clause, "Force Majeure" shall mean an event beyond the control of the parties, due to or as a result of or caused by acts of God, wars, insurrections, riots, Pandemics, earthquake and fire, events not foreseeable but does not include any fault or negligence or carelessness on the part of the parties, resulting in such a situation.

In the event of any such intervening Force Majeure, each party shall notify the other party in writing of such circumstances and the cause thereof immediately within five calendar days. Unless otherwise directed by the other party, the party pleading Force Majeure shall continue to perform/render/discharge other obligations as far as they can reasonably be attended/fulfilled and shall seek all reasonable alternative means for performance affected by the Event of Force Majeure.

In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of three months, the parties shall hold consultations with each other in an endeavour to find a solution to the problem. Notwithstanding the above, the decision of UIIC shall be final and binding on the Bidder.

21 DISPUTE RESOLUTION

The bids and any contract resulting there from shall be governed by and construed according to the Indian Laws. All settlement of disputes or differences whatsoever, arising between the parties out of or in connection to the construction, meaning and operation or effect of this Offer or in the discharge of any obligation arising under this Offer (whether during the course of execution of the order or after completion and whether before or after termination, abandonment or breach of the Agreement) shall be resolved amicably between UIIC and the vendor's representative.

In case of failure to resolve the disputes and differences amicably within 30 days of the receipt of notice by the other party, then the same shall be resolved as follows:

"Any dispute or difference whatsoever arising between the parties out of or relating to the construction, meaning, scope, operation or effect of this contract or the validity or the breach thereof shall be settled by arbitration in accordance with the Rules of Arbitration of the Indian Council of Arbitration and the award made in pursuance thereof shall be binding on the parties."

The venue of the arbitration shall be Chennai.
The language of arbitration shall be English.
The award shall be final and binding on both the parties.

Work under the contract shall be continued by the vendor during the arbitration proceedings unless otherwise directed in writing by UIIC unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator is obtained. Save as those which are otherwise explicitly provided in the contract, no payment due, or payable by UIIC, to the vendor shall be withheld on account of the ongoing arbitration proceedings, if any, unless it is the subject matter, or one of the subject matters thereof.

Sole arbitrator to be jointly appointed by both parties. The cost of arbitration shall be borne equally by both the parties.

22 WAIVER

No failure or delay on the part of any of party relating to the exercise of any right power privilege or remedy provided under the this tender and the subsequent agreement with the other party shall operate as a waiver of such right, power, privilege or remedy or as a waiver of any preceding or succeeding breach by the other party nor shall any single or partial exercise of any right, power, privilege or remedy preclude any other or further exercise of such or any other right, power privilege or remedy provided in this tender and subsequent agreement all of which are several and cumulative and are not exclusive of each other or of any other rights or remedies otherwise available to either party at law or in equity unless such waiver , amendments or modification is in writing and signed by the party against whom enforcement of the waiver, amendment or modification is sought.

23 TERMINATION

UIIC shall be entitled to terminate the agreement/purchase order with the Bidder at any time giving 60(sixty) days prior written notice to the Bidder if the Bidder breaches its obligations under the tender document or the subsequent agreement/purchase order and if the breach is not cured within 30 (Thirty) days from the date of notice.

24 TERMINATION FOR CONVENIENCE

UIIC may terminate the Contract, in whole or in part, at any time for its convenience by written notice of not less than 60 (sixty) days. The notice of termination shall specify that termination is for the UIIC's convenience, the extent to which performance of the Vendor under the Contract is terminated, and the date upon which such termination becomes effective. The Bidder needs to make sure that during transition needs to be done as per the agreed methodology and time between UIIC and bidder. The transition period should be guided by the Exit Management clause of the RFP.

25 CONTRACT/AGREEMENT

The contract/agreement between the Vendor and the Purchaser will be signed in accordance with all the terms and conditions mentioned in this tender document and addendums/corrigendum.

The successful bidder must furnish two copies of the contract/agreement in ₹100/- stamp paper, with all the above terms and conditions mentioned including the commercials. The draft of the contract/agreement will be shared to the successful bidder along with the LOA.

The successful bidder must furnish the duly signed contract/agreement along with the security deposit/performance guarantee for UIIC's counter signature within 15 days from the receipt of LOA.

PROJECT TIMELINES

The Bidder is expected to adhere to these timelines stipulated below. Non-compliance to these timelines by the Bidder would lead to Liquidated Damages as stated in this RFP.

Hardware Refresh Timeline		
S#	**Key Activities**	**Timeline**
1	Submission of Project Plan - Detailing each task with target date and assigned resources including migration plan of existing infrastructure from old equipment to New equipment and installation of all items supplied and integration with existing infrastructure at DC and DR.	T+1 Week
2	Delivery of Hardware at DC & DR	T+12 Weeks
3	Power-on, Basic Installation and configuration of all items supplied at DC and DR Sites'	T+13 Weeks
4	Completion of all work at DC and DR Sites' including migration, commissioning and documentation.	T+17 Weeks

*T: T is the date of issuance of Purchase Order

NOTE:

a. UIIC, at its discretion, shall have the right to alter the project schedule based on the implementation plan. This will be communicated formally to the Bidder during the implementation, if a need arises.
b. The Bidder is required to provide a detailed strategy to UIIC; the activities mentioned above are indicative but the timelines for procurement and delivery should be maintained. Hence if the Bidder has a faster and more effective solution the same may be discussed and agreed by UIIC.
c. Any delay in the above timelines may attract delivery penalties as Mentioned in Service Level agreement section
d. After the delivery is made, if it is discovered that the items supplied are not according to our specification, such supply would be rejected at the supplier's cost.

26 WARRANTY, ON-SITE MAINTENANCE, AMC, ATS:

Hardware / Software Acceptance: - UIIC will carry out the acceptance tests for testing of software, hardware and verification that the supplied components are as per bill of material through UIIC appointed consultant / UIIC Team. The Bidder shall assist UIIC in all acceptance tests to be carried out by UIIC. Bidder needs to rectify all the gaps highlighted in the Acceptance testing without any additional cost to UIIC

Hardware / Software Go-Live: - The respective hardware and software will be termed as Go-live only when the application for which the hardware is allocated goes in production and all the data is migrated.

The Bidder shall undertake to provide an onsite comprehensive 03 (THREE) Year Warranty and AMC for next 02 (two) years (Back-to-Back with OEM) for all supplied hardware commencing from the date of Go-live and acceptance of Hardware for all supplied Hardware commencing from the date of commissioning at the respective delivered locations of the Company as provided in the Purchase Order / Contract for Supply.

Replacement under warranty clause shall be made by the Supplier free of all charges at site including freight, insurance, and other incidental charges.

The Bidder shall undertake to provide an onsite comprehensive 03 (THREE) Year Warranty and ATS for next 02 (two) years (BACK-TO-BACK with OEM) for all supplied Software commencing from the date of Go-Live and sign off by UIIC of the software for the respective delivered locations of the Company as provided in the Purchase Order / Contract for Supply.

The bidders shall quote AMC/ATS Charges for the solution for a period of 2 years after the initial comprehensive onsite warranty period of 3 years in the commercial bid.

ATS/AMC rates to be quoted for the post warranty period must for a support similar to the one extended during warranty period with OEM back-to-back support.

27 PERIOD OF CONTRACT

Contract period shall be for five-years (3-year warranty and 2-year AMC) from date of acceptance of purchase order.

SCHEDULE OF REQUIREMENT

S#	Item Description	HW/SW	Quantity	Warranty (In Years)	Support (In years)
1.	HCL Domino Complete collaboration, 12-month S&S renewal, authorized user	SW	15000	ATS For 5-year period w.e.f. 01.09.2022	
2.	HCL Sametime complete, 12-month S&S renewal, authorized user	SW	1500	ATS For 5-year period w.e.f. 01.09.2022	
3.	Bulk Mailing solution	SW	1 lac bulk e-mails per day	For 5-year period	
4.	Verified Mark certificate (VMC)	SW	1 domain (uiic.co.in)	For 5-year period	
5.	DMARC	SW	1 domain (uiic.co.in)	For 5-year period	
6.	Gateway level S/MIME	SW	1 domain (uiic.co.in)	For 5-year period	
7.	Mobile Device Management	SW	2000	3	2
8.	HCI Nodes + External Storage	HW	5 at DC, 5 at DR	3	2
9.	Virtualisation Infrastructure, operations	SW	For entire HCI	3	2
10.	Backup, Archival and Journal licenses	SW	15000 @ DC 15000 @ DR	3	2
11.	E-discovery licenses	SW	15000 @ DC	3	2
12.	Email Security Gateway	SW	15000 @ DC 15000 @ DR	3	2
13.	HIPS	SW	For all HCI workloads	3	2
14.	Operating System licenses	SW	For all HCI Workloads	3	2

28 PAYMENT TERMS

a. No advance payment shall be made in any case.
b. All payments will be made to the Bidder in Indian Rupees only.
c. AMC & ATS charges shall be paid yearly in advance after the warranty period.
d. The Bidder recognizes that all payments to the Bidder under this RFP and subsequent agreement are linked to and dependent on successful achievement and acceptance of deliverables / activities set out in the project plan and therefore any delay in achievement of such deliverables / activities shall automatically result in delay of such corresponding payment.
e. Any objection / dispute to the amounts invoiced in the bill shall be raised by UIIC within reasonable time from the date of receipt of the invoice.
f. All out of pocket expenses, travelling, boarding and lodging expenses for the entire term of this RFP and subsequent agreement is included in the amounts and the Bidder shall not be entitled

to charge any additional costs on account of any items or services or by way of any out-of-pocket expenses, including travel, boarding and lodging etc.

g. The company also reserves the right to prescribe additional documents for release of payments and the bidder shall comply with the same.

h. The bidder shall cover the entire scope of services mentioned and deliver all the 'deliverables' as mentioned under the scope of work.

i. The bidder must accept the payment terms proposed by UIIC. The financial bid submitted by the bidder must be in conformity with the payment terms proposed by UIIC. Any deviation from the proposed payment terms would not be accepted. UIIC shall have the right to withhold any payment due to the SP, in case of delays or defaults on the part of the SP. Such withholding of payment shall not amount to a default on the part of UIIC.

Hardware:

- 70% on total hardware price on delivery on production of proof of delivery / delivery challan.
- Balance 30% of total hardware price on project sign off, with supporting documents.

Software:

- 50% of software price on delivery of the software licenses.
- Balance 50% of total software price on project sign off.
- Bulk email charges shall be paid quarterly in arrears.

Implementation Charges:

- 50% of Implementation charges on completion of implementation of the solution, complete data migration from the existing solution to newly installed solution.
- Balance 50% of total Implementation charges on project sign off.

Facility Management Services (FMS):

- FMS payment shall be paid on quarterly basis at the end of each quarter after performance review of the solution.

AMC/ATS:

- AMC of hardware and ATS of software support shall be paid quarterly in advance post completion of warranty period after deducting applicable penalties.

Successful bidder has to submit the OEM support certificate for all Products, Hardware, Software and deliverables for releasing the payment. UIIC will not release the payment until the certificate from the OEM will not be provided. UIIC shall pay each undisputed invoice raised in accordance with this RFP and subsequent agreement, within thirty (30) Days after its receipt unless otherwise mutually agreed in writing, provided that such invoice is dated after such amount have become due and payable under this RFP and subsequent agreement. Any objection / dispute to the amounts invoiced in the bill shall be raised by the UIIC within 21 days from the date of receipt of the invoice, only in exceptional circumstances will UIIC raise a dispute beyond 21 days. Upon settlement of disputes with respect to any disputed invoice(s), the UIIC will make payment within thirty (30) Days of the settlement of such disputes.

29 DELAY IN BIDDER'S PERFORMANCE

Delivery/installation/migration/commissioning of in scope equipment's and software at DC/DR/NDR & Chennai HO shall be made by the bidder in accordance with the time schedule specified by UIIC in the contract. Any delay by the bidder in the performance of action relating to implementation/service/other obligations shall render the bidder liable to any or all of the following sanctions:

- Forfeiture of performance security,
- Imposition of liquidated damages,
- Termination of the contract for default.

30 INSPECTION OF RECORDS

All work under or in course of execution or executed in pursuance of the contract shall at all times be open to the inspection and supervision of the company as well as the company's authorized representatives and the contractor shall at all times during the usual working hours and at all other times at which reasonable notice of the intention of the company or company's representatives to visit the works have been given to the contractor, either himself be present or receive order or instructions or have a responsible agent duly accredited in writing present for that purpose.

Said records are subject to examination. UIIC's auditors would execute confidentiality agreement with the bidder, provided that the auditors would be permitted to submit their findings to UIIC, which would be used by UIIC. The cost of the audit will be borne by UIIC. The scope of such audit would be limited to Service Levels being covered under the contract, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities.

31 RIGHTS OF VISIT

UIIC reserves the right to inspect and monitor/assess the progress of the project at any time during the course of the Contract. The Purchaser may demand and upon such demand being made, the Purchaser shall be provided with any document, data, material or any other information, which it may require, to enable it to assess the progress of the project.

32 CLARIFICATION TO BIDDERS

All queries / requests for clarification from bidders must reach us by e-mail to (rfp.email@uiic.co.in) before due date mentioned in *Section 1 - Bid Schedule and Address as* per Annexure 12 – Prebid Query format only. No clarifications or queries will be responded in any other format. Any changes in the tender document shall be uploaded in the UIIC website / e-tender website only.

The text of the clarifications sought (without identifying the source of enquiry) and the response given by UIIC, together with amendment / corrigendum to the bidding document, if any, will be posted on UIIC website (https://uiic.co.in) / e-tender portal only. It would be responsibility of the bidder to check the website and e-tender portal (https://uiic.enivida.com/) before final submission of bids.

33 EVALUATION METHODOLOGY

The evaluation will be a conducted in the following stages:

1. Eligibility Bid Evaluation;
2. Technical Bid Evaluation;
3. Commercial Bid evaluation.

The objective of evolving this evaluation methodology is to facilitate the selection of the most optimal solution that appropriately meets the business requirements of the UIIC. The bidders would be screened based on the General Eligibility Criteria. Post qualification of a Bidder on these criteria, bid would be evaluated on its technical soundness. All bids shall be evaluated by an Evaluation Committee set up for this purpose by the UIIC. The evaluation shall be on the basis of quality of the solution & services offered and cost of the offered solution and services. Bidder's qualifying the technical bid evaluation will be considered for commercial evaluation.

The decision of the UIIC would be final and binding on all the Bidders to this document. UIIC may accept or reject an offer without assigning any reason whatsoever.

General Eligibility Criteria

UIIC shall scrutinize the Eligibility bid submitted by the bidder. A thorough examination of supporting documents to meet each eligibility criteria shall be conducted to determine the Eligible bidders. Bidders not complying with the eligibility criteria are liable to be rejected and shall not be considered for Technical Evaluation.

The bidders meeting the General Eligibility Criteria will be considered for technical evaluation. Any credential/supporting detail mentioned in "Annexure 6- Eligibility criteria form" and not accompanied by relevant proof documents will not be considered for evaluation. All credential letters should be appropriately bound, labelled, and segregated in the respective areas. There is no restriction on the number of credentials a Bidder can provide.

Technical Bid Evaluation

The Technical Proposals of only those bidders shall be evaluated who have satisfied the eligibility criteria bid. UIIC may seek clarifications from the any or each bidder as a part of technical evaluation. All clarifications received by within stipulated time shall be considered for evaluation. In case a clarification is not received within the stipulated time, the respective technical parameter would be treated as non-compliant and decision to qualify the bidder shall be accordingly taken by the UIIC.

Commercial Bid Evaluation

The commercial bid of only those bidders shall be opened who have been technically qualified on the basis of the technical proposal.

The envelope containing the Commercial offers of only those Bidders, who are short-listed after technical evaluation, would be opened. The format for quoting commercial bid set out in Annexure 7. The commercial offer should consist of comprehensive Cost for required solution. Bidder must provide detailed cost breakdown, for each category mentioned in the commercial bid. UIIC will determine whether the Commercial Bids are complete, unqualified and unconditional. Omissions, if any, in costing any item shall not entitle the firm to be compensated and the liability to fulfil its obligations as per the Scope of the RFP within the total quoted price shall be that of the Bidder.

Commercial Bid Evaluation Considerations

Commercial bid evaluation shall be considered as below in case of any kind of discrepancy:

1. If there is a discrepancy between words and figures, the amount in words shall prevail
2. If there is a discrepancy between percentage and amount, the amount calculated as per the stipulated percentage basis shall prevail
3. Where there is a discrepancy between the unit rate and the line item total resulting from multiplying the unit rate by the quantity, the unit rate will govern unless, in the opinion of UIIC, there is an obvious error such as a misplacement of a decimal point, in which case the line item total will prevail
4. Where there is a discrepancy between the amount mentioned in the bid and the line item total present in the schedule of prices, the amount obtained on totalling the line items in the Bill of Materials will prevail
5. The amount stated in the correction form, adjusted in accordance with the above procedure, shall be considered as binding, unless it causes the overall price to rise, in which case the bid price shall prevail
6. If there is a discrepancy in the total, the correct total shall be arrived at by UIIC
7. In case the bidder does not accept the correction of the errors as stated above, the bid shall be rejected.
8. At the sole discretion and determination of the UIIC, the UIIC may add any other relevant criteria for evaluating the proposals received in response to this RFP.
9. All liability related to non-compliance of this minimum wages requirement and any other law will be responsibility of the bidder.
10. The UIIC shall not incur any liability to the affected bidder on account of such rejection.
11. The commercials will be calculated till two decimal points only. If the third decimal point is greater than .005, the same shall be scaled up else it shall be scaled down to arrive at two decimal points. UIIC will make similar treatment for 4th or subsequent decimal point to finally arrive at two decimal points only.

34 AT RISK AMOUNT

The quarterly At-Risk Amount ('ARA') shall be 15% of the estimated quarterly pay-out of the respective month. In case maximum penalty is imposed for more than two times in a year, UIIC will impose an additional penalty of 5% of the quarterly charges and may consider termination of services.

Overall cap for penalties as per SLA and the Liquidated damages over the tenure of the contract will be 10% (ten per cent.) of the contract value

35 Make IN INDIA

Guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order) vide GOI, Ministry of Commerce and Industry, Department of Industrial Policy and Promotion Notification No.P45021/2/2017(BE-II) dated June 15, 2017 and revision thereto and Ministry of Electronics and Information Technology vide Notification no F.No 33 (1)/2017/IPHW dated 14th September 2017 will be applicable for this RFP and allotment will be done in terms of said Order(s), if applicable, for any of the equipment.

36 Subcontracting

Bidder shall not subcontract or permit anyone other than its personnel to perform any of the work, service or other performance required of the bidder under the contract. Compliance to SLA will be the bidder's responsibility.

ANNEXURE 1- Format for Letter of Authorisation

(To be submitted in the Bidder's letter head)

[To be included in 'Cover – A' Eligibility Bid Envelope]

Ref. No: 000100/HO IT/RFP/734/2021-2022

To
The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, NALANDA
19,4th Lane
Uthamar Gandhi Salai,
(Nungambakkam High Road)
Chennai – 600034

LETTER OF AUTHORISATION FOR ATTENDING BID OPENING

The following persons are hereby authorized to attend the bid opening on _____(date) in respect of the tender for "REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION" on behalf of M/s._____ (Name of the Bidder) in the order of preference given below:

Order of Preference Name Designation Specimen Signature

1.

2.

(Authorized Signatory of the Bidder)

Date:

(Company Seal)

1. Maximum of two persons can be authorized for attending the bid opening.
2. Permission for entry to the hall where bids are opened may be refused in case authorization as prescribed above is not submitted.

ANNEXURE 2- No Blacklist Declaration

(To be submitted in the Bidder's letterhead)

[To be included in 'Cover – A' Eligibility Bid Envelope]

Ref. No: 000100/HO IT/RFP/734/2021-2022

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, NALANDA
19,4th Lane
Uthamar Gandhi Salai,
(Nungambakkam High Road)
Chennai – 600034

Subject: Submission of No Blacklisting Self-Declaration for Tender Ref. No: 000100/HO IT/RFP/734/2021-2022 "REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

Dear Sir/Madam,

We do hereby declare and affirm that we have not been blacklisted/debarred by any Government Departments, Agencies or Public Sector Undertakings in India as on the date of submission of the tender for "REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

(Authorized Signatory of Bidder)

Date:
(Company Seal)

ANNEXURE 3 – Manufacturers' Authorisation Format (MAF)

(To be submitted on OEMs Letter Head)

[To be included in 'Cover – A' Eligibility Bid Envelope]

Ref. No: 000100/HO IT/RFP/734/2021-2022

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office, NALANDA,
19,4th Lane
Uthamar Gandhi Salai,
(Nungambakkam High Road)
Chennai – 600034

Subject: Manufacturers Authorisation Form for the "Tender for Proposal (RFP) for REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

<This MAF should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its eligibility bid>

MAF should broadly cover the following:

a. Registered office address of OEM
b. Authorizing bidder to participate in the tender and negotiate and conclude the contract with UIIC.
c. Confirm extension of full warranty and guarantee as per the terms and conditions of the tender and the contract for the solution, products/equipment and services including extension of technical support and updates / upgrades if contracted by the bidder
d. ensure all product upgrades including software upgrades and new product feature releases during the contract period.
e. And also confirm that such Products as UIIC may opt to purchase from the Supplier, provided, that this option shall not relieve the Supplier of any warranty obligations under the Contract.
f. In the event of termination of production of such Products:

   i. advance notification to UIIC of the pending termination, in sufficient time to permit the UIIC to procure needed requirements; and

   ii. Following such termination, furnishing at no cost to UIIC, the blueprints, design documents, operations manuals, standards and specifications of the Products, if requested.

g. Should also confirm to undertake, that in case if the bidder is not able to maintain the solution to the satisfaction of the Company as per the functional and technical specification of the bid, will replace the bidder with another bidder to maintain the solution till the contract period in this bid at no extra cost to the company.

Yours faithfully,

(Authorized Signatory of Bidder)

Date:

(Company Seal)

ANNEXURE 4 – Statement of Nil Deviations

(To be submitted in the Bidder's letterhead)

[To be included in 'Cover – A' Eligibility Bid Envelope]

Ref. 000100/HO IT/RFP/734/2021-2022

To
The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office NALANDA, # 19,4th Lane
Uthamar Gandhi Salai,
(Nungambakkam High Road)
Chennai – 600034

Re: Your RFP Ref. 000100/HO IT/RFP/734/2021-2022 - "Tender for Proposal (RFP) for SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

Dear Sir,

This is to confirm that we have submitted a no deviation bid and unconditionally accept all requirements, payment terms, integrity pact, SLAs, Scope and the terms and conditions as mentioned in the said RFP including all corrigendum/amendment floated by United India Insurance Co. Ltd. pertaining to Selection of System Integrator for Supply, Installation and maintenance of Hardware and supplied software at DC and DR. Any assumption or exclusion submitted by us in the proposal which are contradictory to the RFP or subsequent corrigendum/amendment stands null and void.

Yours faithfully,

(Authorized Signatory of Bidder)

Date:
(Company Seal)

ANNEXURE 5 – Bank Guarantee Format For EMD

To
The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd
Head Office, NALANDA, # 19,4th Lane
Uthamar Gandhi Salai,
(Nungambakkam High Road)
Chennai – 600034

Whereas..... (Hereinafter called "the Bidder") has submitted its bid dated..... (Date of submission of bid) for the "REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION "(hereinafter called "the Bid"), we..... (Name of Bank), having our registered office at..... (Address of bank) (Hereinafter called "the Bank"), are bound unto United India Insurance Co. Ltd (hereinafter called "the Purchaser") for the sum of ₹ 3,30,00,000/-(Rupees Three Crore and Thirty lakhs only) for which payment well and truly to be made to the said Purchaser, the Company binds itself, its successors, and assigns by these presents.

THE CONDITIONS of this obligation are:

- If the Bidder/System Integrator withdraws his offer after issuance of letter of acceptance by UIIC;
- If the Bidder/System Integrator withdraws his offer before the expiry of the validity period of the tender
- If the Bidder/System Integrator violates any of the provisions of the terms and conditions of this tender specification.
- If a Bidder/System Integrator, who has signed the agreement and furnished Security Deposit backs out of his tender bid.
- If a Bidder/System Integrator having received the letter of acceptance issued by UIIC, fails to furnish the bank guarantee and sign the agreement within the 15(Fifteen) days from the letter of acceptance.

We undertake to pay the Purchaser up to the below amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it, owing to the occurrence of all/any of the above conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including ninety (90) days from last date of bid submission, and any demand in respect thereof should reach the Company not later than the above date. Notwithstanding anything contained herein:

1. Our liability under this bid security shall not exceed ₹ 25,00,000/-
2. This Bank guarantee will be valid upto ..... (Date);
3. We are liable to pay the guarantee amount or any part thereof under this

Bank guarantee only upon service of a written claim or demand by you on or before ..... (Date).

In witness whereof the Bank, through the authorized officer has set its hand and stamp on this.....day of .....at .....

(Signature of the Bank)

NOTE:

1. Bidder should ensure that the seal and CODE No. of the authorized signatory is put by the bankers, before submission of the bank guarantee.
2. Bank guarantee issued by banks located in India shall be on a Non-Judicial Stamp Paper of appropriate value.
3. Bid security should be in INR only.
4. Presence of restrictive clauses in the Bid Security Form such as suit filed clause/ requiring the Purchaser to initiate action to enforce the claim etc., will render the Bid non- responsive.

Unsuccessful bidders' bid security will be discharged or returned after the expiration of the period of bid validity prescribed by the Company.

The successful bidder's bid security will be discharged upon the bidders signing the contract and furnishing the performance bank guarantee.

ANNEXURE 6 – Eligibility Criteria

[To be included in 'Cover – A' Eligibility Bid Envelope]

To

The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd
Head Office, NALANDA, # 19,4th Lane
Uthamar Gandhi Salai,
(Nungambakkam High Road)
Chennai – 600034

Ref. 000100/HO IT/RFP/734/2021-2022

ELIGIBILITY CRITERIA FOR BIDDERS

S#	Particulars	
1	Registered Name & Address of The Bidder	
2	Location of Corporate Head Quarters	
3	Date & Country of Incorporation	
4	GSTIN and date of registration	
5	In the Location business since (year)	
6	Whether the bidder is an OEM / SI	
7	Address for Communication	
8	Contact Person-1 (Name, Designation, Phone, Email ID)	
9	Contact Person-2 (Name, Designation, Phone, Email ID)	

TURN OVER & NET PROFIT

Financial Year / Accounting Year	Turnover (in Crores)	Net Profit
2018-2019		
2019-2020		
2020-2021		

S#	Eligibility Criteria for Bidders	Documentary Proof Required
1.	The Bidder should be a Registered Company in India under the 'Companies Act' and should be in existence in India for more than five (05) years as on 31.12.2021.	Copy of the Certificate of Incorporation issued by Registrar of Companies.
2.	The bidder should be authorized by the OEMs of the proposed equipment/devices and solution to bid for this tender.	MAF as per annexure 3 for Authorised partner. Self-declaration if the bidder is an OEM.
3.	The bidder should have an average annual financial turnover of at least ₹ 50 Crore for the last three financial year's viz. 2018-19, 2019-20, and 2020-21.	Audited financial statements / Certificate from Auditor

4.	The bidder should have made Net Profit after taxation in one of the last three financial years viz. 2018-19, 2019-20, and 2020-21.	Audited financial statements / Certificate from Auditor
5.	The bidder should not have been blacklisted/ debarred by any Government Departments, Agencies or Public Sector Undertakings in India as on the date of submission of the tender	As per annexure 2: No Blacklist declaration
6.	Bidder should have its own Support center for Telephonic and Remote Assistance Services in Chennai, Mumbai / Navi Mumbai & Hyderabad	Self-Declaration along with the details of the support centers in Chennai, Mumbai / Navi Mumbai & Hyderabad.
7.	As per the Government guidelines on Procurement bidder needs to submit the Annexure 14	Bidder needs to Submit Annexure 14 on letter head dully signed by Authorized signatory.
8.	Pre-Integrity Pact	Bidder needs to submit to copies of Pre-Integrity Pact as per Annexure 11.

Note:

1. In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
2. Bidders need to ensure compliance to all the eligibility criteria points.
3. Scheduled commercial banks do not include regional rural banks and cooperative banks.
4. Scheduled commercial banks refer to public sector / scheduled commercial banks in India only.
5. Branches mentioned are per bank / insurance company and are not cumulative across banks / insurance companies.
6. Either the bidder representing a principal/OEM of the proposed solution or Principal/OEM itself can bid but both cannot bid simultaneously for the same product in this tender.
7. If a bidder submits bid on behalf of the principal/OEM, the same bidder shall not submit on behalf of another principal/OEM in this tender
8. The branches being considered in the criteria should be per Bank / Insurance and not cumulative across Banks.
9. In case of business transfer where bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired Business may be considered.
10. We furnish hereunder the details of Demand Draft submitted towards RFP document fees and Earnest Money Deposit.

Description	**Amount in INR**	**Name of issuing bank and branch**	**UTR NO/BG NO**
Cost of Bid Document	25,000		
EMD	25,00,000		

Yours faithfully,

(Authorized Signatory of Bidder)

Date:

(Company Seal)

ANNEXURE 7 – Commercial Bid Format

[To be included in Cover 'C'- Commercial Bid]

RFP Ref. 000100/HO IT/RFP/734/2021-2022 - "Tender for Proposal (RFP) for SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

1. Name of the Bidder :

2. Address of Corporate Office :

TABLE I – Cost of Solution

S#	Description	Qty (a)	Unit Price (b)	Total Price (a*b)
1.a	Bulk Mailing solution with 3 years comprehensive onsite warranty.	1 crore emails per quarter		
1.b	Verified Mark certificate (VMC) with 3 years comprehensive onsite warranty.	1 domain (uiic.co.in)		
1.c	DMARC with 3 years comprehensive onsite warranty.	1 domain (uiic.co.in)		
1.d	Gateway level S/MIME with 3 years comprehensive onsite warranty.	1 domain (uiic.co.in)		
1.e	Mobile Device Management with 3 years comprehensive onsite warranty.	2000		
1.f	HCI Nodes + External Storage with 3 years comprehensive onsite warranty.	5 at DC, 5 at DR		
1.g	Virtualisation Infrastructure, operations with 3 years comprehensive onsite warranty.	For entire HCI		
1.h	Backup, Archival and Journal licenses with 3 years comprehensive onsite warranty.	15000 @ DC 15000 @ DR		
1.i	E-discovery licenses with 3 years comprehensive onsite warranty.	15000 @ DC		
1.j	Email Security Gateway with 3 years comprehensive onsite warranty.	15000 @ DC 15000 @ DR		
1.k	HIPS with 3 years comprehensive onsite warranty.	For all HCI workloads		
1.l	Operating System licenses with 3 years comprehensive onsite warranty.	For all HCI workloads		
2.	**Total Cost**			

TABLE II – Cost of Implementation

S#	Description	Qty	Total Price
2.a	Charges, if any, for carrying out all the implementation activities and migration as per the Scope of Work. (IMPLEMENTATION, MIGRATION CHARGES AND OTHERS IF ANY)		
2.	**Total Cost**		

TABLE III – AMC for Hardware

S#	Description	Qty (a)	Unit Price (b)	Total Price (a*b)
3.a	AMC for Hardware for 4th year	5 at DC, 5 at DR		
3.b	AMC for Hardware for 5th year	5 at DC, 5 at DR		
2.	**Total Cost**			

TABLE IV – ATS for Licenses / Software

S#	Description	Qty (a)	Unit Price (b)	Total Price (a*b)
4.a	ATS for Bulk Mailing solution for 4th year.	1 crore emails per quarter		
4.b	ATS for Bulk Mailing solution for 5th year.	1 crore emails per quarter		
4.c	ATS for Verified Mark certificate (VMC) for 4th year.	1 domain (uiic.co.in)		
4.d	ATS for Verified Mark certificate (VMC) for 5th year.	1 domain (uiic.co.in)		
4.e	ATS for DMARC for 4th year.	1 domain (uiic.co.in)		
4.f	ATS for DMARC for 5th year.	1 domain (uiic.co.in)		
4.g	ATS for Gateway level S/MIME for 4th year	1 domain (uiic.co.in)		
4.h	ATS for Gateway level S/MIME for 5th year	1 domain (uiic.co.in)		
4.i	ATS for MDM for 4th year	2000		
4.j	ATS for MDM for 5th year	2000		
4.k	ATS for Virtualisation Infrastructure, operations for 4th year	For entire HCI		
4.l	ATS for Virtualisation Infrastructure, operations for 5th year	For entire HCI		
4.m	ATS for Backup, Archival and Journal licenses for 4th year	15000 @ DC 15000 @ DR		
4.n	ATS for Backup, Archival and Journal licenses for 5th year	15000 @ DC 15000 @ DR		
4.o	ATS for E-discovery licenses for 4th year	15000 @ DC		

4.p	ATS for E-discovery licenses for 5th year	15000 @ DC		
4.q	ATS for Email Security Gateway for 4th year	15000 @ DC 15000 @ DR		
4.r	ATS for Email Security Gateway for 5th year	15000 @ DC 15000 @ DR		
4.s	ATS for HIPS for 4th year.	For all HCI workloads		
4.t	ATS for HIPS for 5th year.	For all HCI workloads		
4.u	ATS for OS license cost for 4th year	For all HCI workloads		
4.v	ATS for OS license cost for 5th year	For all HCI workloads		
2.	**Total Cost**			

TABLE V – Cost of Onsite Support (1st to 5th Year)

S#	Description	Monthly Cost (a)	No of Months (b)	Cost of Support (a*b)
5.a	Cost of onsite support for 1st year		12	
5.b	Cost of onsite support for 2nd year		12	
5.c	Cost of onsite support for 3rd year		12	
5.d	Cost of onsite support for 4th year		12	
5.e	Cost of onsite support for 5th year		12	
2.	**Total Cost**			

TABLE VI – Total Cost of Ownership (TCO)

S#	Description	Table	Total Price
A.	Total amount under serial no. 2	Table I	
B.	Total amount under serial no. 2	Table II	
C.	Total amount under serial no. 2	Table III	
D.	Total amount under serial no. 2	Table IV	
E.	Total amount under serial no. 2	Table V	
F.	**GRAND TOTAL**		

Rate Card

S#	Description	Qty (a)	Unit Price (b)	Total Price (a*b)
1.	Bulk Mailing solution	2 crore emails per quarter		
2.	Bulk Mailing solution	3 crore emails per quarter		
3.	Bulk Mailing solution	4 crore emails per quarter		
4.	Bulk Mailing solution	5 crore emails per quarter		

Note:

1. All amount should be in INR only.
2. All software supplied under this bid shall be of enterprise class with OEM support.
3. Bidders should ensure that the volume pricing mentioned in the rate card is less than or equal to the price quoted in the TCO by the bidder in the bid.
4. If the cost for any line item is indicated as zero, then it will be assumed by the company that the said item is provided to the company without any cost.
5. The prices quoted above shall be considered for all the deliverables stated in this RFP document. No extra costs other than those quoted above shall accrue to the company.
6. L1 will be determined based on the total cost of ownership (TCO).
7. PO shall be placed for the TCO value only (mentioned in Table VI) and Rate card shall be utilized based on UIIC requirements during the contract period.
8. We certify that the items quoted above meet all the Technical specifications, Functional requirements, Technical requirements as per Annexure 9 of the RFP.

Further, we declare that all the terms and conditions as per the Bid document were read by us and we are agreeable to all the terms and conditions.

Authorised Signature:

Name:

Designation:

Date:

ANNEXURE 8- Non Disclosure Agreement (NDA)

(To be submitted in separate ₹100 stamp paper)
[To be included in 'Cover – A' Eligibility Bid Envelope]

RFP Ref. 000100/HO IT/RFP/734/2021-2022 - "Tender for Proposal (RFP) for SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

This confidentiality and non-disclosure agreement is made on the.....day of....., 20..... between (Bidder), (hereinafter to be referred to as "-------") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns a company incorporated under the Companies Act, 1956 and having its principal office at .....(address) and UNITED INDIA INSURANCE COMPANY LIMITED (hereinafter to be called "UIIC") which expression shall unless repugnant to the subject or the context mean and included its successors, nominees or assigns having its Registered Office at ..... (address) on the following terms and conditions:

WHEREAS, in the course of the business relationship between the aforesaid parties, both the parties acknowledge that either party may have access to or have disclosed any information, which is of a confidential nature, through any mode and recognize that there is a need to disclose to one another such confidential information, of each party to be used only for the Business Purpose and to protect such confidential information from unauthorized use and disclosure;

NOW THEREFORE, in consideration of the mutual promises contained herein, the adequacy and sufficiency of which consideration is hereby acknowledged and agreed, the parties hereby agree as follows:

This Agreement shall apply to all confidential and proprietary information disclosed by one party to the other party, including information included in the caption 'Definitions' of this Agreement and other information which the disclosing party identifies in writing or otherwise as confidential before or within thirty days after disclosure to the receiving party ("Confidential Information"). Information may be in any form or medium, tangible or intangible, and may be communicated/disclosed in writing, orally, electronically or through visual observation or by any other means to one party (the receiving party) by the other party (the disclosing party).

1. DEFINITIONS

(a) CONFIDENTIAL INFORMATION means all the information of the Disclosing Party which is disclosed to the Receiving party pursuant to the business arrangement whether oral or written or through visual observation or in electronic mode and shall include but is not limited to trade secrets, know-how, inventions, techniques, processes, plans, algorithms, software programs, source code, semiconductor designs, schematic designs, business methods, customer lists, contacts, financial information, sales and marketing plans techniques, schematics, designs, contracts, financial information, sales and marketing plans, business plans, clients, client data, business affairs, operations, strategies, inventions, methodologies, technologies, employees, subcontractors, the contents of any and all agreements, subscription lists, customer lists, photo files, advertising materials, contract quotations, charity contracts,

documents, passwords, codes, computer programs, tapes, books, records, files and tax returns, data, statistics, facts, figures, numbers, records, professionals employed, correspondence carried out with and received from professionals such as Advocates, Solicitors, Barristers, Attorneys, Chartered Accountants, Company Secretaries, Doctors, Auditors, Surveyors, Loss Assessors, Investigators, Forensic experts, Scientists, Opinions, Reports, all matters coming within the purview of Privileged Communications as contemplated under Indian Evidence Act, 1872, legal notices sent and received, Claim files, Insurance policies, their rates, advantages, terms, conditions, exclusions, charges, correspondence from and with clients/ customers or their representatives, Proposal Forms, Claim-forms, Complaints, Suits, testimonies, matters related to any enquiry, claim-notes, defences taken before a Court of Law, Judicial Forum, Quasi-judicial bodies, or any Authority, Commission, pricing, service proposals, methods of operations, procedures, products and/ or services and business information of the Disclosing Party. The above definition of Confidential Information applies to both parties equally; however, in addition, without limitation, where the Disclosing Party is the UIIC, no information that is exempted from disclosure under section8 or any other provision of Right to Information Act, 2005 shall at any time be disclosed by the Receiving Party to any third party.

(b) MATERIALS means including without limitation, documents, drawings, models, apparatus, sketches, designs and lists furnished to the Receiving Party by the Disclosing Party and any tangible embodiments of the Disclosing Party's Confidential Information created by the Receiving Party.

2. COVENANT NOT TO DISCLOSE

The Receiving Party will use the Disclosing Party's Confidential Information solely to fulfil its obligations as part of and in furtherance of the actual or potential business relationship with the Disclosing Party. The Receiving Party shall not use the Confidential Information in any way that is directly or indirectly detrimental to the Disclosing Party or its subsidiaries or affiliates and shall not disclose the Confidential Information to any unauthorized third party. The Receiving Party shall not disclose any Confidential Information to any person except to its employees, authorized agents, consultants and contractors on a need-to-know basis, who have prior to the disclosure of or access to any such Confidential Information agreed in writing to receive it under terms at least as restrictive as those specified in this Agreement.

In this regard, the agreement entered between the Receiving Party and any such person/s shall be forwarded to the Disclosing Party promptly thereafter. Prior to disclosing any Confidential Information to such person/s, the Receiving Party shall inform them of the confidential nature of the information and their obligation to refrain from disclosure of the Confidential Information. The Receiving party shall use at least the same degree of care in safeguarding the Confidential Information as it uses or would use in safeguarding its own Confidential Information and shall take all steps necessary to protect the Confidential Information from any unauthorized or inadvertent use. In no event shall the Receiving Party take all reasonable measures that are lesser than the measures it uses for its own information of similar type. The Receiving Party and its Representatives will immediately notify the Disclosing Party of any use or disclosure of the Confidential Information that is not authorized by this Agreement. In particular, the Receiving Party will immediately give notice in writing to the Disclosing Party of any unauthorized use or disclosure of the Confidential Information and agrees to assist the Disclosing Party in remedying such unauthorized use or disclosure of the Confidential Information.

The Receiving Party and its Representatives shall not disclose to any person including, without limitation any corporation, sovereign, partnership, company, Association of Persons, entity or individual
(i) the fact that any investigations, discussions, or negotiations are taking place concerning the actual or potential business relationship between the parties,
(ii) that it has requested or received Confidential Information, or
(iii) any of the terms, conditions, or any other fact about the actual or potential business relationship.

This confidentiality obligation shall not apply only to the extent that the Receiving Party can demonstrate that:

(a) the Confidential Information of the Disclosing Party is, or properly became, at the time of disclosure, part of the public domain, by publication or otherwise, except by breach of the provisions of this Agreement; or

(b) was rightfully acquired by the Receiving Party or its Representatives prior to disclosure by the Disclosing Party.

(c) was independently developed by Receiving Party or its Representatives without reference to the Confidential Information; or

(d) the Confidential Information of the Disclosing Party is required to be disclosed by a government agency, is the subject of a subpoena or other legal or demand for disclosure; provided, however, that the receiving party has given the disclosing party prompt written notice of such demand for disclosure and the receiving party reasonably cooperates with the disclosing party's efforts to secure an appropriate protective order prior to such disclosure.

(e) is disclosed with the prior consent of or was duly authorized in writing by the disclosing party.

3. RETURN OF THE MATERIALS

Upon the disclosing party's request, the receiving party shall either return to the disclosing party all Information or shall certify to the disclosing party that all media containing Information have been destroyed. Provided, however, that an archival copy of the Information may be retained in the files of the receiving party's counsel, solely for the purpose of proving the contents of the Information.

4. OWNERSHIP OF CONFIDENTIAL INFORMATION

The Disclosing Party shall be deemed the owner of all Confidential Information disclosed by it or its agents to the Receiving Party hereunder, including without limitation all patents, copyright, trademark, service mark, trade secret and other proprietary rights and interests therein, and Receiving Party acknowledges and agrees that nothing contained in this Agreement shall be construed as granting any rights to the Receiving Party, by license or otherwise in or to any Confidential Information. Confidential Information is provided “as is” with all faults.

By disclosing Information or executing this Agreement, the disclosing party does not grant any license, explicitly or implicitly, under any trademark, patent, copyright, mask work protection right, trade secret or any other intellectual property right.

In no event shall the Disclosing Party be liable for the accuracy or completeness of the Confidential Information. THE DISCLOSING PARTY DISCLAIMS ALL WARRANTIES REGARDING THE INFORMATION, INCLUDING ALL WARRANTIES WITH RESPECT TO INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS AND ALL WARRANTIES AS TO THE ACCURACY OR UTILITY OF SUCH INFORMATION. Execution of this Agreement and the disclosure of Information pursuant to this Agreement does not constitute or imply any commitment, promise, or inducement by either party to make any purchase or sale, or to enter into any additional agreement of any kind.

5. REMEDIES FOR BREACH OF CONFIDENTIALITY

(a) The Receiving Party agrees and acknowledges that Confidential Information is owned solely by the disclosing party (or its licensors) and that any unauthorized disclosure of any Confidential Information prohibited herein or any breach of the provisions herein may result in an irreparable harm and significant injury and damage to the Disclosing Party which may be difficult to ascertain and not be adequately compensable in terms of monetary damages. The Disclosing Party will have no adequate remedy at law thereof, and that the Disclosing Party may, in addition to all other remedies available to it at law or in equity, be entitled to obtain timely preliminary, temporary or permanent mandatory or restraining injunctions, orders or decrees as may be necessary to protect the Disclosing Party against, or on account of, any breach by the Receiving Party of the provisions contained herein, and the Receiving Party agrees to reimburse the reasonable legal fees and other costs incurred by Disclosing Party in enforcing the provisions of this Agreement apart from paying damages with interest at the market rate prevalent on the date of breach to the Disclosing Party.

(b) The Receiving Party agrees and acknowledges that any disclosure, misappropriation, conversion or dishonest use of the said Confidential Information shall, in addition to the remedies mentioned above, make the Receiving Party criminally liable for Breach of Trust under section 405 of the Indian Penal Code.

6. TERM

This Agreement shall be effective on the first date written above and shall continue in full force and effect at all times thereafter. This Agreement shall however apply to Confidential Information disclosed by the Disclosing Party to the Receiving Party prior to, as well as after the effective date hereof. The Receiving Party acknowledges and agrees that the termination of any agreement and relationship with the Disclosing Party shall not in any way affect the obligations of the Receiving Party in not disclosing of Confidential Information of the Disclosing Party set forth herein. The obligation of non-disclosure of Confidential Information shall bind both parties, and also their successors, nominees and assignees, perpetually.

7. GOVERNING LAW & JURISDICTION

This Agreement shall be governed by and construed with solely in accordance with the laws of India in every particular, including formation and interpretation without regard to its conflicts of law provisions.

Any proceedings arising out of or in connection with this Agreement shall be brought only before the Courts of competent jurisdiction in Chennai.

8. ENTIRE AGREEMENT

This Agreement sets forth the entire agreement and understanding between the parties as to the subject-matter of this Agreement and supersedes all prior or simultaneous representations, discussions, and negotiations whether oral or written or electronic. This Agreement may be amended or supplemented only by a writing that is signed by duly authorized representatives of both parties.

9. WAIVER

No term or provision hereof will be considered waived by either party and no breach excused by the Disclosing Party, unless such waiver or consent is in writing signed by or on behalf of duly Constituted Attorney of the Disclosing Party. No consent or waiver whether express or implied of a breach by the Disclosing Party will constitute consent to the waiver of or excuse of any other or different or subsequent breach by the Receiving Party.

10. SEVERABILITY

If any provision of this Agreement is found invalid or unenforceable, that part will be amended to achieve as nearly as possible the same economic or legal effect as the original provision and the remainder of this Agreement will remain in full force.

11. NOTICES

Any notice provided for or permitted under this Agreement will be treated as having been given when (a) delivered personally, or (b) sent by confirmed telecopy, or (c) sent by commercial overnight courier with written verification of receipt, or (d) mailed postage prepaid by certified or registered mail, return receipt requested, or (e) by electronic mail, to the party to be notified, at the address set forth below or at such other place of which the other party has been notified in accordance with the provisions of this clause. Such notice will be treated as having been received upon actual receipt or five days after posting. Provided always that notices to the UIIC shall be served on the Information Technology Department of the Company's Head Office at Chennai and a CC thereof be earmarked to the concerned Branch, Divisional or Regional Office as the case may be by RPAD & email.

IN WITNESS WHEREOF THE PARTIES HERE TO have set and subscribed their respective hands and seals the day and year herein above mentioned.

(a) for & on behalf of United India Insurance Co. Ltd DEPUTY GENERAL MANAGER	(a) for & on behalf of (BIDDER'S NAME)
In the presence of: Witnesses - 1: Witnesses - 2:	In the presence of: Witnesses - 1: Witnesses - 2:

ANNEXURE 9 – Minimum Functional & Technical Specifications

[To be included in Cover 'B' - Technical Bid Envelope]

S#	Minimum Technical Specification parameter	Compliance (Yes/No)
BULK MAILING SOLUTION		
1.	Proposed solution should have provision to provide Dashboard to track the usage of consumption.	
2.	Proposed solution should have provision to give information related to Suppression list.	
3.	Proposed solution should have provision to do Campaign Management with detailed management as in who opened or clicked your campaigns, how many times and from what location and device.	
4.	Proposed solution should have provision to incorporate API, with public IP of the bulk mailing solution provider.	
5.	Proposed solution should have provision to provide template editor.	
6.	Proposed solution should have provision to import/export Subscribers list, reports, stats etc.	
7.	Proposed solution should have provision to process automatic email bounce processing, blacklisting engine and feedback loop support.	
8.	Proposed solution should have provision to manage Subscriber & provide Subscribers segmentation.	
9.	Solution should be able to manage multiple contact list, add or import contacts, unsubscribe link, unlimited custom fields, export of contacts etc.	
10.	Solution should have following features to email design like - Upload or Import Content, Easily upload images, Free Email Templates, Email Personalization, Advanced HTML Editing, Anchor Links, Unsubscribe Link etc.	
11.	Solution should have the option of "send now or later" and monitoring of "link click tracking" etc.	
12.	Solution should have features like email newsletter, drag and drop editor, HTML templates, Email automation, signup forms, subscriber management, subscriber segmentation etc.	
VERIFIED MARK CERTIFICATE (VMC)		
1.	Supplier must issue VMC certificate from one of the reputed CA such as Digicert, Entrust etc.	
2.	Product should be able to provide guidance with regards to Certificate Authority Authorization (CAA) compliance.	
3.	All outbound emails shall have the verified logo implemented.	
DMARC		
1.	Proposed solution should have provision to block Email Phishing in Real Time.	
2.	Proposed solution should have provision to secure Unlimited passive domain at no additional cost.	
3.	There should not be any limitation/upper capping on outgoing emails tracking/unlimited outgoing email protection for the domain DMARC is bought for.	
4.	Proposed solution should have provision to get Aggregate reports (RUA).	
5.	Proposed solution should have provision to get Forensic Report (RUF) If required.	
6.	Proposed solution should have provision to give complete details of IP Reputation, Blacklisting and whois.	
7.	Proposed solution should have provision to check IP Threat Intelligence.	

8.	Proposed solution should have provision to validate Email sources and must be able to done the pre-validation of SPF.	
9.	Proposed solution should have provision to identify threats by Maps and geography wise.	
10.	Proposed solution should have provision to provide descriptive Custom reports including IP reputation, DMARC journey from None to Reject, Top senders etc.	
11.	Proposed solution should have provision to incorporate 2FA.	
12.	Proposed solution should have provision to provide notification from Look-a-like domains.	
13.	Proposed solution should have provision to provide complementary 4 simulations attacks per year.	
GATEWAY LEVEL SMIME		
1.	PKI Platform should be able to Encrypt and secure confidential communications.	
2.	PKI Platform should be able to Easily authenticate user access via a web-based application or extranet portal.	
3.	Should be able to provide same key pair on all the end-user devices.	
4.	It should support PKI client/ Self-support portal/ OS/browser enrollment methods.	
5.	It should support Automated configuration via PKI client with gateway and AD authentication.	
6.	It should support Automated configuration via passcode.	
7.	It should support Automatic deployment of certificates to domain-joined machines via Windows Group Policy Object (GPO), with Active Directory (AD) integrations, or Light Directory Active Directory (LDAP).	
8.	Seamless integration with third-party tools.	
9.	Should be able to perform Two-part recovery.	
MOBILE DEVICE MANAGEMENT		
1.	Enroll mobile devices with over-the-air enrollment and leverage zero touch provisioning for corporate devices, self-enrolment.	
2.	Enroll mobile devices over the air using self-enrollment for BYOD devices.	
3.	Deploy mobile apps and control app installation.	
4.	Solution should allow management of all endpoints like iOS, Android, Windows, Linux, macOS and Unix systems through a centralised console.	
5.	Solution should support 15,000 endpoints without any additional hardware for application servers. However UIIC proposes to obtain 2000 only with an option to use the same price for additional users on-boarded at a later date as per UIIC discretion.	
6.	Solution should provide a management dashboard that provides a decluttered view of managed device states and alert administrator about potential issues.	
7.	Solution should be able to report devices that do not have a passcode policy enforced.	
8.	solution should be able to report devices that do not have restrictions applied.	
9.	Solution should be able to report devices that need an OS update.	
10.	Solution should report devices that have not been actively reporting for greater than 24 hours.	
11.	Solution should provide detailed list of policies created and deployed through the system and list of devices targeted by each policy.	
12.	Capability to disable/enable: camera, Wi-Fi, Bluetooth, browser etc.	

13.	Solution should be capable enough to deploy MDM actions and policies to configure, secure devices. E.g Lock, Wipe, Restart, Shutdown, remove policy or Unenroll.	
14.	Solution should be certified to manage Android Work Profile Management, Full Device Management and Dedicated Device Management.	
15.	Solution should allow admins to control patching of mobile devices by disabling the auto patch and allow only specific version to be pushed.	
16.	Restriction policies should be applicable on Applications, Connectivity, Device, Security features of Android and Network Settings.	
17.	Restriction policies should be able to control to allow or block Fingerprint unlock, passcode modification, password sharing etc.	
18.	Solution should create work profile where company approved apps are installed and accessed.	
19.	Solution should not allow data to be transferred between personal and work profile.	
20.	Solution should support complete erase of android devices which are in Fully Managed mode.	
21.	Should allow to wipe, lock, shutdown or restart devices through console.	
22.	Solution should provide an easy way to upload custom policies in different formats like xml, Json, mobileconfig, syncml.	
23.	Solution should be able blacklist of apps in iOS and iPadOS. Shouldn't allow th application to be shown or Launch.	
24.	Solution should report details of the device like Serial Number, Operating System version, Device hardware etc.	
25.	Solution should be able to report management details for devices like Last reported time, Installed Policy name, Installed policy payload like certificates etc. where applicable.	
26.	Solution should provide a simple procedure to create policies for iOS and Android devices and manage the policies as groups for easy deployment to devices.	
27.	Solution should provide a built-in health check capability to identify potential issues with the management system and recommend remedial actions to resolve the identified issues.	
28.	Solution should have strong role-based access control built into the management system to ensure only administrator approved functions can be executed by the management operators of the management system.	
29.	Solution should use Apple (iOS) & Google (Android) specific notification services for instant notification of policy changes to devices across the internet.	
30.	The bidder shall propose Support & Subscription / warranty services for 5 years from direct OEM for 24x7x365 with unlimited incident support including unlimited upgrades and updates.	
HARDWARE		
	Hardware - DC (HCI Nodes + External Storage)	
1.	Minimum 5 Nodes.	
2.	Proposed solution should have Intel Xeon Gold 6238R Cascade Lake CPU or above on each node.	
3.	Minimum 56 Cores per cpu, 2 sockets per node.	
4.	Min. 384 GB DDR4 ECC RAM per Node.	
5.	Node should have separate HDD/SSD for OS (ESXi) installation.	

6.	175 TB of usable space without considering any data reduction features like deduplication & compression. Capacity should be sized using one node failure.	
7.	Should have minimum 6 ports out of which 2 should be 25Gbps FC and other 4 should be 10Gbps FC either all on-board OR PCI-E with sufficient redundancy to function in case of any NIC failures.	
8.	Must be able to sustain 3 NIC port failure per node.	
9.	Each HCI node should have dual-PSU's and must be able to sustain single power supply failure.	
10.	No Single Point of Failure with complete redundancy at all levels. Nodes should be configured to have at least one copy of data available in cluster, in order to support data & cluster availability in event of One Node Failure.	
11.	2 Nos of Network Switches with adequate 10/25 Gbps FC port for TOR Connectivity and uplink to Core.	
12.	The proposed solution should have the usable resources specified even after one node failure in the cluster. All such HA requirements must be factored separately over the provided requirements.	
13.	Enterprise storage with 250TB Usable Capacity backed by sufficient NL-SAS Disks in RAID-6 Configuration and another 100TB Usable capacity backed by SAS Drives in RAID-5 configuration.	
14.	The storage solution should have at least 2 hot spares from each type of disk provided in the storage to be able to rebuild in case of disk failures.	
15.	The storage solution should be factored with licenses to take snapshots & cloning for the entire capacity expected as part of the solution.	
16.	The storage should have a minimum of 4 * 10Gbps iSCSI Target Ports for host connectivity thru the TOR Switches.	
17.	The connectivity (cables, SFP, transceiver etc.) necessary for storage, server and uplink connectivity to the core switch must be proposed as part of the solution by the bidder.	
18.	The proposed solution must be factored under production support for 5 yrs 24 x 7 x 365.	
	Hardware-DR (HCI Nodes + External Storage)	
1.	Minimum 5 Nodes.	
2.	Proposed solution should have Intel Xeon Gold 6238R Cascade Lake CPU or above on each node.	
3.	Minimum 56 Cores per cpu, 2 sockets per node.	
4.	Min. 384 GB DDR4 ECC RAM per Node.	
5.	Node should have separate HDD/SSD for OS (Esxi) installation.	
6.	175 TB of usable space without considering any data reduction features like deduplication & compression. Capacity should be sized using one node failure.	
7.	Should have minimum 6 ports out of which 2 should be 25Gbps FC and other 4 should be 10Gbps FC either all on-board OR PCI-E with sufficient redundancy to function incase of any NIC failures.	
8.	Must be able to sustain 3 NIC port failure per node.	
9.	Each HCI node should have dual-PSU's and must be able to sustain single power supply failure.	
10.	No Single Point of Failure with complete redundancy at all levels. Nodes should be configured to have at least one copy of data available in cluster, in order to support data & cluster availability in event of One Node Failure.	
11.	2 Nos of Network Switches with adequate 10/25 Gbps FC port for TOR Connectivity and uplink to Core.	

12.	The proposed solution should have the usable resources specified even after one node failure in the cluster. All such HA requirements must be factored separately over the provided requirements.	
13.	Enterprise storage with 250TB Usable Capacity backed by sufficient NL-SAS Disks in RAID-6 Configuration and another 100TB Usable capacity backed by SAS Drives in RAID-5 configuration.	
14.	The storage solution should have at least 2 hot spares from each type of disk provided in the storage to be able to rebuild in case of disk failures.	
15.	The storage solution should be factored with licenses to take snapshots & cloning for the entire capacity expected as part of the solution.	
16.	The storage should have a minimum of 4 * 10Gbps iSCSI Target Ports for host connectivity thru the TOR Switches.	
17.	The connectivity (cables, SFP, transceiver etc.) necessary for storage, server and uplink connectivity to the core switch must be proposed as part of the solution by the bidder.	
18.	The proposed solution must be factored under production support for 5 yrs 24 x 7 x 365.	
	Software Defined Storage	
1.	The proposed solution shall provide software-based enterprise class storage services on commodity x86 servers.	
2.	Shared Storage created by clustering server attached traditional magnetic Disks or Flash Disks (like SSDs, NVMes etc.).	
3.	Should provide high-resilient shared storage capacity for Virtual environment.	
4.	Should be configured using either Hybrid disk types or All-Flash Storage.	
5.	Can be integrated with Hypervisor or deployed as an additional VM/Appliance/software.	
6.	Should support nondisruptive Scale-Up (Upgrade by inserting drives in existing empty drive-slots) & Scale-Out (Upgrade by adding nodes) upgrades to grow capacity and/or performance whenever required.	
7.	The solution should provide a single unified management console for the management of the entire environment including virtualized environment as well as software defined storage environment. This would simplify the manageability of the entire solution.	
8.	The proposed solution should support space optimization techniques like deduplication, compression, erasure-coding etc. The licenses / configuration required for the functionality must be included in the solution from day-1.	
9.	The proposed solution must be capable of providing storage capacity to other clusters without any licensing dependencies or impact.	
10.	The networking infrastructure needed for the solution should be proposed as a part of the solution, if required.	
11.	The solution should be in the leader's quadrant of Gartners Magic Quadrant for Hyper-Converged Infrastructure.	
	Hypervisor	
1.	Hypervisor management software console shall provide a single view of all virtual machines, allow monitoring of system availability and performance and automated notifications with email alerts.	
2.	The Hypervisor management software should provide the core administration interface as a single Web based interface. This interface should be flexible and robust and should simplify the hypervisor control through shortcut navigation,	

	custom tagging, enhanced scalability, and the ability to manage from anywhere with Internet Explorer, Firefox, Google Chrome, Opera enabled devices.	
3.	The management software should provide means to perform quick, as-needed deployment of additional hypervisor hosts.	
4.	The Hypervisor should have capability to simplify host deployment and compliance by creating virtual machines from configuration templates.	
5.	Power, storage related, and OS cluster related information has to initiate from the relevant sources and can be integrated through RESTful APIs.	
6.	Hypervisor management software console shall provide reports for performance and utilization of Virtual Machines. It shall co-exist and integrate with leading systems management vendors.	
7.	Hypervisor management software console shall provide capability to monitor and analyse virtual machines, and server utilization and availability with detailed performance graphs.	
8.	Hypervisor management software console shall maintain a record of significant configuration changes and the administrator who initiated them.	
9.	Hypervisor management software console shall provide the Manageability of the complete inventory of virtual machines, and physical servers with greater visibility into object relationships.	
10.	Hypervisor management software should provide a global search function to access the entire inventory of multiple instances of Hypervisor management server, including virtual machines, hosts, data stores and networks, anywhere from within Hypervisor management server.	
11.	Hypervisor management software should support user role and permission assignment (RBAC).	
12.	Hypervisor management software should allow to deploy and export virtual machines.	
13.	Hypervisor management software should allow reliable for Physical/ Virtual machines running Windows and Linux operating systems to virtual environment.	
14.	Hypervisor management software should include provision for automated host upgrade / patch management with no VM downtime.	
15.	Hypervisor management software should be able to integrate into existing standard SPSD systems.	
16.	The management solution for hypervisor should provide Single-Sign-On capability which should dramatically simplify administration by allowing users to log in once to access all instances or layers of management without the need for further authentication.	
17.	The bidder shall propose Support & Subscription services from the direct OEM support 24x7x365 with unlimited incident support and including the unlimited upgrades and updates.	
18.	Hypervisor software shall provide a Hypervisor layer that sits directly on the quoted hardware with no dependence on a general purpose OS for greater reliability and security	
19.	Hypervisor software shall allow heterogeneous support for guest Operating systems like Windows client, Windows Server, Linux (at least Red Hat, SUSE, Ubuntu, CentOS).	
20.	Hypervisor software shall allow taking point-in-time snapshots of the virtual machines to be able to revert back to an older state if required.	

21.	Hypervisor software should have the ability to avoid allocating all storage space upfront. Full monitoring capabilities and alerts to prevent from accidentally running out of physical storage space should be there.	
22.	Hypervisor software should support live Virtual Machine migration between different generations of CPUs in the same cluster and without the need for shared storage option.	
23.	Hypervisor software shall have High Availability capabilities for the virtual machines if in case one server/Node fails all the Virtual machines running on that server shall be able to migrate to another physical server running same Hypervisor software.	
24.	Hypervisor software should have the provision to provide zero downtime, zero data loss and continuous availability for the applications running in virtual machines in the event of physical host failure.	
25.	Hypervisor software should provide integration of 3rd party endpoint security to secure the virtual machines with offloaded antivirus, antimalware solutions with/without the need for agents inside the virtual machines.	
26.	Hypervisor software should allow configuring each virtual machine with one or more virtual NICs. Each of those network interfaces can have its own IP address and even its own MAC address, must support NIC teaming for load sharing and redundancy.	
27.	Hypervisor software shall allow creating virtual switches that connect virtual Machines.	
28.	Hypervisor software shall support configurations of 802.1q VLANs which are compatible with standard VLAN implementations from other vendors.	
29.	Hypervisor software should allow dynamic adjustment of the teaming algorithm so that the load is always balanced across a team of physical network adapters.	
30.	Hypervisor software should provide solution to automate and simplify the task of managing hypervisor installation, configuration and upgrade on multiple physical servers.	
31.	Hypervisor software should support for increasing capacity by adding CPU, Memory or disk to virtual machines on an as needed basis without any disruption in working VMs running windows and Linux operating system.	
32.	It should provide the ability to set constraints that restrict placement of a virtual machine to a subset of hosts in a cluster and to keep virtual machines paired or separated.	
33.	Hypervisor software shall continuously monitor utilization across virtual machines and should intelligently allocate available resources among virtual machines.	
34.	Hypervisor software should provide enhanced visibility into storage throughput and latency of hosts and virtual machines that can help in troubleshooting storage performance issues.	
35.	Hypervisor software shall be able to dynamically allocate and balance computing capacity across collections of hardware resources aggregated into one unified resource pool with optional control over movement of virtual machines like restricting VMs to run on selected physical hosts.	
36.	Hypervisor software should provide proactive High availability capability that utilizes server health information and migrates VMs from degraded hosts before problem occurs.	

37.	Hypervisor software should provide Data at rest encryption protects unauthorized data access.	
38.	It should support hardware as well as non-hardware accelerated 3D graphics to run Basic 3D applications in virtual machines.	
39.	The solution should provide an option to easily deploy and manage big data solutions like HANA, Hadoop & VDI on the Hypervisor platform.	
	Operational and Log Analytics	
1.	The solution shall provide a unified management of performance, capacity and compliance for the proposed platform	
2.	The solution shall support monitoring of all the operating systems part of the proposed platform	
3.	The solution shall provide the ability to identify and report on over-sized, under-sized, idle and powered-off virtual workloads such that the environment can be right-sized and resources can be reclaimed	
4.	The solution shall provide predictive analytics capabilities to understand baselines and model capacity and demand for accurate forecasting of infrastructure requirements	
5.	The solution shall provide alerts with symptoms and recommended actions for known problems with the ability add custom alerts (with symptoms and recommended actions)	
6.	The proposes solution should have out of the box capacity analytics and modelling, with granularity ranging from entire datacenter to cluster to invidividual host level	
7.	The solution should give explanations and recommended solutions to performance, capacity and configuration problems. Associate workflows with Smart Alerts to automatically initiate corrective measures at critical thresholds	
8.	The solution should provide prebuilt and configurable operations dashboards to provide real-time insight into infrastructure behavior, upcoming problems, and opportunities for efficiency improvements	
9.	The solution should provide the ability to integrate data from third-party systems to manage the data-center ecosystem components such as compute, networking, storage proposed.	
10.	The solution should be able to collect and analyze all types of machine-generated log data, for example, application logs, network traces, configuration files, messages, performance data and system state dumps	
11.	The solution should allow connecting to data-center ecosystem components e.g., operating systems, applications, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyze logs at scale	
12.	The solution should provide log analytics to be able to bring unstructured and structured data together, for enhanced end-to-end operations management.	
13.	The solution should be able to deliver real-time monitoring, search, and log analytics, coupled with a dashboard for stored queries, reports, and alerts, enabling correlation of events across the IT environment.	
14.	The solution should enable administrators to connect to everything in their environment, e.g., operating systems, applications, storage arrays, firewalls, network devices, etc., providing a single location to collect, store, and analyze logs at scale	
15.	Should provide vm and host performance monitoring, capacity planning, optimization and compliance reporting.	

16.	Should support alerts with which automated actions can be taken. Should also support dynamic thresholds.	
17.	The solution should have the capability to balance the workloads across the clusters and provide the ability to define the placement policy based on business intent like SLA, compliance, license separation, application tiering etc.	
18.	The capacity model should include costing for effective procurement planning	
19.	The solution should have a comprehensive what-if analysis feature for workload planning, infrastructure planning and migration planning across private and public cloud along with costing	
20.	The solution of should OOTB intuitive dashboards and ability to create custom dashboards which can be shared for cross-team collaboration.	
21.	It should have built-in compliance monitoring for PCI, HIPAA, DISA, FISMA, ISO, CIS for the underlying virtual environment	
22.	The lifecycle of the entire cloud management solution (day-0 and day-2 operations) should be supported and taken care by the solution itself.	
	Configuration & Patch Management	
1.	Should have integrated Configuration management capabilities to build the custom states for complex tasks for OS and Applications.	
2.	Should have capability to automate Software deployment and updates	
3.	Should have inbuilt Patching, orchestrated OS app maintenance and day-2 application deployments to endpoints	
4.	The solution should be highly scalable to manage 1000s of workloads and be able to support agent-based / agentless / proxy-agent based configuration	
5.	The solution should be built on an event driven engine that can detect events arising out a configuration drift, errors, notifications and quickly remediate by enforcing them to the desired state	
6.	The solution should be capable to manage complex orchestration (e.g., multistep system patching and restarts), cross-application workflows, or even business processes, such as updating ITSM, CMDB, or other systems of record.	
	Licensing	
1.	The bidder shall propose Support & Subscription services for 5 years from direct OEM for 24x7x365 with unlimited incident support including unlimited upgrades and updates.	
ARCHIVAL & JOURNALING		
1.	Journal Archival of all the existing emails from HCL Domino Server. This is required for all 15000 users.	
2.	Archival of all existing emails and linking with respective users.	
3.	Archival solution should be able to archive the same user mail box at DC and DR.	
4.	Solution should support user level mailbox archival for all 15000 HCL Domino users.	
5.	The solution should provide the capability to import existing emails from HCL Notes/Domino without requiring conversion to an intermediate form.	
6.	The proposed solution should include data protection to disk and tape.	
7.	License should be included for archival and E-discovery for all users.	
8.	Solution should be capable to archive each mail passing through either email gateway (external) or within the organization (internal).	
9.	Proposed solution should offer integrated E-discovery capabilities for all users.	
10.	The solution should allow for integration with LDAP/AD.	

11.	Proposed solution should support content indexing for EML, HTM, HTML, LOG, MSG, TXT, XML, XMIND.	
12.	The solution should provide role-based access – admins, users, auditors etc.	
13.	Solution should provide role-based web interface and search capabilities and download options.	
14.	Solution should be capable to archive non-email content such as Calendar, Contacts and notes in user level mailbox archival.	
15.	Solution should be capable to retrieve the archive data from HCL Notes client as well as Web based GUI.	
16.	Solution should provide Domino integration. Through this integration, one should be capable to see ones archived email in same folder structure as maintained on email server. Plugin should also provide the search capability.	
17.	Solution should have de-duplication and encryption ability for archived data.	
18.	Solution should have ability to scan files for viruses, spyware, and malware before archival.	
19.	Solution should be able to be configured in cluster mode with more than 01 archiver solution at different geographical locations. Cluster should work in HA mode.	
20.	Bidder should include all necessary software to run the solution.	
21.	Proposed backup solution should support integration with proposed archival solution for consistent copy.	
22.	Bidder should also provide all necessary hardware and software for proposed solution	
23.	Solution should be able to integrate with LDAP services such as Active Directory.	
24.	Solution should also provide facility to create local users with configurable access controls.	
25.	Solution should have predefined role built-in and administrator should have capability to assign these roles to any user.	
26.	Solution should provide the facility of granular access controls for user to restrict their access to undesired data.	
27.	Solution should provide comprehensive reports on various user activities, storage utilization and projection of storage growth.	
28.	Proposed solution should be a leader in Gartner magic quadrant.	
29.	The bidder shall propose Support & Subscription / warranty services for 5 years from direct OEM for 24x7x365 with unlimited incident support including unlimited upgrades and updates.	
BACKUP SOLUTION		
1.	Proposed backup solution should be configured to support On-Premises backup for the HCL Domino Messaging System. Solution should be able to backup data of all the aforementioned applications from same solution instance and separate solution for different backup should not be quoted by the vendor.	
2.	The solution should provide functionality to perform daily and unattended scheduled automatic backups of data available in HCL Domino Server.	
3.	Proposed backup Solution should be licensed to cover all mailboxes. Proposed licensing metric should not restrict based on storage requirement for backup of data.	
4.	The solution should support upgradation of storage at a later stage of time for supporting backup of additional data.	

5.	If User based licensing is proposed for the backup solution, UIIC should have the flexibility to re-assign licenses when the licensed user exits the UIIC on grounds of Retirement, Resignation, etc. The data of such mail boxes to be retained as per the retention policy of the UIIC and should not be deleted on reassignment of licenses.	
6.	The backup solution should support de-deduplication of data.	
7.	The solution must have alert generation facility through e-mail/SMS in case of any issue during the backup process.	
8.	Should have in-built frequency and calendar-based scheduling system.	
9.	The proposed backup solution should be capable of backing up Group Mailboxes without the need for additional licenses.	
10.	The proposed backup solution should support granularity in backups, i.e., it should be capable to include/exclude items from the backups.	
11.	The proposed backup solution should provide complete security and efficiency of data protection by leveraging global deduplication, encryption, compression, and WAN-optimized replication.	
12.	The proposed backup solution should have capability in additional security using 2FA / MFA for the backup application console to restrict un-authorized access to the backup management console.	
13.	The proposed backup solution should support backup consistency checks for guaranteed data recovery. The solution should have the option to run these tests on daily, weekly, monthly and the latest backups.	
14.	The proposed backup solution should support replication of the backups to a DR site, and it should be capable of exporting specific backups to the DR servers or even to widely used public or private clouds.	
15.	The proposed backup solution should easily restore HCL Domino data (nsf files, server config files etc.) back to the any of the available Lotus Server in case information was intentionally or accidently deleted.	
16.	The software should be able to generate logs & report e.g. de-duplication report, Data growth analysis report, Compute utilization report during backup etc.	
17.	The solution must support Unlimited retention for the backed up data.	
18.	The solution should support role-based Access restriction. It should be able to integrate with UIIC existing AD for authentication.	
19.	Solution should be able to have flexibility of Storage target options like SAN, NAS, DAS, Object Storage, etc.	
20.	Flexible backup scheduling with customizable backup settings for backup frequency and backup window.	
21.	UIIC requires that all data be encrypted in transit and at rest.	
22.	Mass recovery of multiple mailboxes should be available in a single restore job.	
23.	UIIC should have the flexibility to perform granular search with Advanced options like multiple search criteria and attributes/ context-based search options (eg. from, subject, name, creation date, etc.) Provides advanced search filter capability for items across multiple users.	
24.	UIIC should have the capability to access reports for a) Licensing compliance or consumption statistics. b) Backup success and failure. c) Ad hoc and scheduled reporting facilities.	
25.	The proposed solution should be able to integrate with existing Tape library / Storage to tape-out/ backup the backed up data. The backup should support Full copy as well as Incremental copy of the data, if required by UIIC.	

26.	The IT Infra to be sized in such a way that the performance of the solution does not degrade during the entire contract period. In case of any degradation in performance, the SI has to upgrade the IT Infra at no additional cost during the contract period.	
27.	Proposed backup solution shall have Web Based GUI which provides intuitive workflows and efficient navigation without traveling across several pages, so most operations can be performed from a single screen.	
28.	Should have ability to set quotas on client owner's computers to limit the data to be backed up.	
29.	Solution provided should have horizontal scalability, allowing client indexes / de-duplication / search indexes and storage resources to scale across multiple servers and storage targets respectively and yet preserve single logical pool of resources for transparent and quick recovery.	
30.	Data Management Master server should be configured in High availability mode, ensuring failure of one server does not affect backup and recovery operations in the setup.	
31.	The solution should support upgradation of storage at a later stage of time for supporting backup of additional data.	
32.	Should support software based de-duplication to support any storage system, cloud repository and object storage as de-duplicated disk target (Software should be Hardware Agnostic with Physical/Virtual/Cloud Support). It should be tightly integrate with backup solution to provide in-line or source-side variable block level deduplication to achieve highest storage reduction methods for backup data retention.	
33.	The proposed solution should be a Leader in Gartner Magic Quadrant for Enterprise Backup software. Bidder shall share the backup design and architecture.	
34.	Should support in built ransomware protection & should support immutable backup architecture without any additional tools.	
35.	The bidder shall propose Support & Subscription / warranty services for 5 years from direct OEM for 24x7x365 with unlimited incident support including unlimited upgrades and updates.	
EMAIL SECURITY GATEWAY		
1.	The solution must support the following enterprise deployment options, cloud, hybrid and on-premises with virtual or physical appliances.	
2.	The solution must provide protection from the following email threats and common nuisances, such as imposter email, phishing, malware, spam, bulk (gray), adult and low-priority mail.	
3.	The solution must have the ability to scale without any issue.	
4.	The solution must provide an advanced message tracing feature.	
5.	The solution must provide real-time reports for detailed visibility into mail flow and trends.	
6.	All end-user services of the solution must be white labelled to provide familiarity for the end users.	
7.	The solution must leverage at least 2 mail transfer agents (MTAs) for incoming and outgoing emails to allow the solution accept and process a large number of concurrent email connections.	
8.	The solution must support integration with external data stores (e.g. LDAP directories) and databases to provide enhanced functionality.	
9.	The solution must recursively unpack compressed and zipped files.	

10.	The solution must provide the connection throttling.	
11.	The solution must provide the capability to mitigate the chance of a denial of service (DoS) attack.	
12.	The solution must provide mechanism(s) for protection from directory harvest attacks.	
13.	The solution must provide protection against inbound and outbound spam.	
14.	The solution must provide a 100% known virus catch rate.	
15.	The solution must have the ability to select from more than 1 anti-virus engines.	
16.	The solution must support detection of Business Email Compromise (BEC) and impostor emails through machine learning technology besides static rulesets.	
17.	The solution must provide spam classifiers (such as adult, bulk mail, impostor, malware, phish, suspected spam, etc.) to enable a more granular policy.	
18.	The solution must provide Circle of Trust email classifier to protects a small group of users which are high-value targets or executives in an Organization from unwanted email from unfamiliar senders.	
19.	The solution must detect malformed SMTP packets.	
20.	The solution must provide the ability to fine-tune spam levels.	
21.	The solution must provide the capability to drop SMTP connections at the connection level based on reputation.	
22.	The solution must provide the ability to detect new spam campaigns in almost real-time.	
23.	The solution must provide cloud-based sandbox service to detect malicious/unknown and new attacks with attachments and URLS.	
24.	The proposed solution must protect the organization against advanced email threats - including zero-day threats, ransomware, polymorphic malware, weaponized documents, and credential phishing attacks.	
25.	The proposed solution must be able to hold messages until a verdict is received from sandbox analysis. Messages should not be sent without attachment or with a reconstructed version of the attachment which loses functionality to avoid sandboxing.	
26.	The proposed solution must be able to immediately quarantine messages with known malicious URLs, and rewrite all other URLs in order to track and block clicks.	
27.	The proposed solution must be able to perform time of click analysis to prevent access to the site if a benign URL goes bad at a later time.	
28.	The proposed solution must be able to perform time of click analysis to allow access to the site via native browser isolation in the case the site verdict cannot be reached for a defined group of people. This capability must follow users regards of corporate device vs. BYOD and whether they are ON or OFF the network, without requiring any driver/app installation.	
29.	The proposed solution must be able to use a combination of static and dynamic technology to apply multi-stage analysis to inspect the entire attack chain.	
30.	The proposed solution must be able to provide predictive analysis to pre-emptively identify and sandbox suspicious URLs based on email traffic patterns.	
31.	The proposed solution must catch threats that leave no obvious digital traces, such as credential phishing attacks.	
32.	The proposed solution must be able to have the ability to prevent malware from evading detection by recognizing evasive attacker techniques.	
33.	The proposed solution must incorporate and leverage a platform of community-based intelligence that spans across email, network, mobile apps,	

	and social media vectors, as well as verified threat intelligence beyond domains and IP addresses.	
34.	The proposed solution must have the ability to be configured with a maximum duration to hold a message prior to delivery.	
35.	The proposed solution must generate alerts on any message that may have been delivered, but retrospectively is detected as malicious.	
36.	The proposed solution should have 99% of messages scanned and released within 3 to 5 minutes.	
37.	The proposed solution must have the ability to manually move all instances of malicious emails out of the user's inbox including cc, bcc, forwarded mails as well as expand distribution lists into a quarantine mailbox to prevent users from opening or clicking on it. This functionality must support HCL Domino Onprem solution.	
38.	The proposed solution must dynamically add a tag to inbound messages to warn or inform users that an incoming message may be dangerous. Tags are added to an incoming message based upon results from the content scan engines.	
39.	The solution must detect lower-volume targeted phishing attacks.	
40.	The solution must allow the customer to create custom phishing rules.	
41.	The solution must create a repository of display names for users in their Organization who are most likely to be targeted for an impostor attack. Permitted email addresses should be limited to external addresses that a legitimate source may use to send inbound email to your Organization.	
42.	The solution must allow administrator to export and import the Impostor Display Names List in CSV file format.	
43.	The solution should provide a phishing reporting button, automated analysis and remediation workflow to allow for automatic retrieval of missed phishing emails when the user reports on it.	
44.	The proposed solution must make use of a combination of static and dynamic detection techniques.	
45.	The proposed solution must be able to include targeted attack attribution information to allow the improvement of contextual understanding of attacks.	
46.	The proposed solution must use big-data analysis and machine-learning heuristics to identify malicious URLs accurately.	
47.	The proposed solution must look at a "normalized" version of the URL in the scoring engine.	
48.	The proposed solution must be able to provide pre-emptive sandboxing before the user gets a chance to click on them.	
49.	The proposed solution must be able to re-write URLs in order to track and block clicks at click time.	
50.	The proposed solution must be able to rewrite scheme-less URLs within emails.	
51.	The proposed solution must be able to provide the granularity to choose whether to re-write URLs within text or HTML message bodies.	
52.	The proposed solution must be able to automatically move all instances of emails with malicious URLs being delivered to all users inbox including cc, bcc and forwarded instances into a quarantine mailbox to prevent users from clicking on it based on the URL sandboxing verdict.	
53.	The proposed solution must be able to create unique policies for URL rewrite policies to different groups of users or members of a Sub-Org.	

54.	The proposed solution must be able to show the original destination visible to the user by hovering over the rewritten URL while message displays the original URL.	
55.	The proposed solution must be able to provide the option to seamlessly integrate with URL browser isolation platform when the user clicks on a rewritten link in the email body, it gets redirected to the isolation environment where the user is free to scroll through the page but cannot upload or download and do any keystroke until a benign verdict is returned from the platform, the user is then allowed to exit the isolation environment.	
56.	The proposed solution must be able to provide Plain Text Option for URL rewrite to appends the domain to the URL label.	
57.	The proposed solution must be able to execute and observe commonly exploited file attachments such as MS office and PDF documents to identify suspicious behavior that indicates the presence of advanced malware.	
58.	The proposed solution must be able to hold messages until a verdict is received after analysis.	
59.	The proposed solution must be able to encrypt all attachments sent to the sandboxing environment and ensure that no customer data is sent in clear text.	
60.	The proposed solution must be able to permit the use of the hash value of attachments as a filter value to search logs.	
61.	The proposed solution must be able to scan the email body content to heuristically use the content to open the password protected documents.	
62.	The solution must have the capability for flexible, policy-based, conditional expression-based filtering and message routing using header and message body values.	
63.	The solution must have the ability to modify SMTP header values, such as to add/remove x-headers, subject line modifications, address rewriting, etc.	
64.	The solution must offer multiple disposition such as attachment stripping, delivery of notices to senders and quarantine of the whole email.	
65.	The solution must apply specific rules on email containing password-protection or encrypted files.	
66.	The solution must have the ability to append keywords to the subject line based on a ruleset.	
67.	The solution must assign different rulesets based on specific email addresses.	
68.	The solution must have the capability to enable BATV tagging by domain or by policy, including when to apply the BATV tagging in the message routing.	
69.	The solution must support granular policies for Sender Policy Framework (SPF), Domain Keys Identified Mail (DKIM), and Domain Message Authentication Reporting & Conformance (DMARC).	
70.	The solution must have the capability to perform recipient verification against Active Directory and other email list source.	
71.	The solution must be able to remove existing DKIM signatures and resign outbound messages for any number of domains and keys.	
72.	The solution must not only enforce DMARC but also report to the vendor's DMARC platform.	
73.	The solution must be able to verify DMARC policy is configured correctly and enforce it.	
74.	The solution must support Authenticated Received Chain (ARC) validation for trusted domain sets for third party sender use cases where DMARC authentication might fail.	

75.	The solution must have message quarantine capabilities.	
76.	The solution must organize messages into separate customer defined quarantine folders.	
77.	The solution must have a distributed quarantine architecture to cater for any unexpected downtime.	
78.	The solution must allow administrator to view, re-route, or release messages in the quarantine.	
79.	The solution must allow end users to receive quarantine digest mails and access the end user quarantine to release messages. All release of mails must be logged.	
80.	The solution must provide a separate quarantine folder for Phishing mails without allowing any access by the end users.	
81.	The solution must have the ability for administrators to preview quarantined messages to determine further actions to be taken.	
82.	The solution must have the ability to selectively route messages or copies of emails to other internal or external destinations, including options to send the email as an attachment, options for tagging the message with custom content or filter/policy status or score, etc.	
83.	The solution must support inserting one or more legal or compliance footers (e.g. disclaimers) in outbound or inbound email.	
84.	The solution must selectively be applied based on policy / attribute or not apply if the email is s/mime encrypted or digitally signed, etc.	
85.	The solution must support multi-languages in the signature/disclaimers.	
86.	The solution must apply signatures and disclaimers based on AD user groups.	
87.	The solution must have the ability to insert dynamic content in the signatures/disclaimers such as date and time, etc.	
88.	The solution must generate spam digests and the duration of the digest emails must be configurable.	
89.	The solution must allow end users to release messages, manage their own safe and block lists and report false negatives and positives direct from the spam digest mail.	
90.	The solution must support all the reporting of false negative and false positive emails.	
91.	The solution must support SAML authentication for end users and administrators.	
92.	The solution must change the color of the login screen, the header for the management interface, and the title for the web-UI.	
93.	The solution must allow administrator to change the maximum limit to the number of messages to be included in email Digests.	
94.	The solution must include a web-based management and configuration console without the need for any plug-ins or add-ons.	
95.	The solution must support role-based and delegated administration.	
96.	The solution must support authentication again the local user data store, an LDAP or active directory source, or via the organization's own identity provider (via SAML).	
97.	The solution must provide administrators with facilities for email queue management.	
98.	The solution must limit the size of the email messages that may be sent/received and/or the number of recipients in an email.	

99.	The solution must limit SMTP probing and check the validity of envelope information before accepting a message for delivery.	
100.	The proposed solution must be able to provide specific information about which users have received and/or clicked on URLs in suspicious emails.	
101.	The proposed solution must restrict logins from specified IP addresses or CIDR blocks of addresses.	
102.	The proposed solution must dynamically create a group of very attacked people group, with the option to further restrict their browsing experience into an isolated container till they have been removed from the very attacked people list.	
103.	The solution must provide support for both RSYSLOG and HTTP based API log ingestion to SIEM for all MTA and filtering logs (supporting both will provide more flexibility with different SIEM providers).	
104.	The solution must provide event driven API for integration with SIEM for events such as missed message containing malicious URL/Attachment, malicious URL clicked and permitted etc.	
105.	The solution must include a message-tracing capability to facilitate help desk work.	
106.	The solution must provide policies for auditing of incoming and outgoing messages.	
107.	The solution must have detailed and summary reporting capabilities as well as the options to schedule reports for email delivery.	
108.	The proposed solution must be able to provide malware campaign intelligence and forensic reports.	
109.	The proposed solution must be able to provide granular reporting for URL time of click events.	
110.	The proposed solution must provide the capability to retain a local copy of security events and metadata of exchanged emails for forensic activities.	
111.	The proposed solution must provide the capability to monitor a list of VIP users within the organization against possible display name spoofing attacks.	
112.	The proposed solution must be able to provide the capability to monitor a list of VIP users within the organization against advanced threats and provide notifications in the event a VIP is being targeted.	
113.	The proposed solution must be able to provide the capability to monitor the attack indexes of personnel that has been targeted and also drill down into what are the threats that are targeting them.	
114.	The proposed solution must be able to provide the capability to list the very attacked persons within an organization to allow the security team to focus efforts on those that are targeted.	
115.	The solution must be able to apply DLP functionality on email policy: It should have inbuilt functionality besides end user classification including image detection and embedded text on image. Prevent data loss and leakage when data is modified, copied, pasted, printed, or transmitted while enabling its flexible use. It should also have facility for forensic analysis capability. It Should have real-time monitoring capability. It should have capability to identify high risk user.	
116.	The solution must provide a centralized and consolidated overview of DLP activity across the Organization with custom views of DLP reports and an incident manager console.	

117.	The solution must allow administrators and security practitioners to view real-time DLP statistics and trends as well as manage current incidents. Data must be able to view in high-level reports or as detailed incidents.	
118.	The solution must allow administrators to assign a status, add comment, review the messages or change the status of an incident for tracking purposes.	
119.	The solution must allow administrators to organize DLP Incidents into specific folders.	
120.	The solution must allow administrators to encrypt the contents of a DLP Incident folder.	
121.	The solution must provide pre-defined dictionaries and Smart Identifiers to scan email messages and attachments and allow administrators to create or modify rules to support compliance with many other types of information privacy and data security regulations.	
122.	The solution must be able to provide a browser-based interface for users to decrypt, read, compose, reply to, and forward encrypted messages to external parties.	
123.	The solution must allow users to manage all of their encrypted messages from one centralized inbox in a web- based portal, instead of opening encrypted messages individually from their regular inbox.	
124.	The solution must allow encryption keys to be managed separately from the content user's encrypt. Keys are generated on the proposed solution and stored on a centralized key server separately.	
125.	The solution must be able to send notification directly to the sender's manager for action, to act upon the message according to organization's security policies, when messages trigger Data Loss Prevention rules.	
126.	The solution must be able to change the original email Subject for the encrypted message notification with a generic or customized Subject. The original Subject will always be displayed when the user views the actual message in the web-based portal.	
127.	The solution must be able to select unique encryption protocol versions for inbound and outbound SMTP traffic since inbound requirements can be more restrictive than outbound requirements.	
128.	Email Encryption Service should be provided for 15,000 users or mailboxes.	
129.	Solution should have dynamic screening capability to block connections that exhibit suspicious activity, such as failing too many authentication attempts, connecting too many times in each frame, attempting to keep a connection too long, or sending to too many invalid recipients.	
130.	Solution should detect account hijack like an user's device cannot be authenticated perpetually and should be able to set a period after which a user's device must be reauthenticated.	
131.	Solution should have IP shielding security feature that only honors SMTP sessions claiming to be from someone at the listed domains if they are coming from an IP address associated with that domain.	
132.	Solution should have backscatter protection	
133.	Solution should have Ransomware, Malware protection and Location screening etc.	
134.	Solution should be patched with Log4j protection.	
135.	Solution should have image detection technique for blocking if found to be suspicious.	

136.	Solution should have domain protection capability.	
137.	Solution should have reputation filtering and anti-spoofing.	
138.	Solution should offer gray mail protection.	
139.	In the event of failure of cloud gateway, alternate solution to be provided by the bidder at no additional cost to UIIC.	
140.	Solution should have all layers of security checks for internal email communication as well, with an option of on demand disabling.	
141.	The bidder shall propose Support & Subscription / warranty services for 5 years from direct OEM for 24x7x365 with unlimited incident support including unlimited upgrades and updates.	
HOST INTRUSION PREVENTION SYSTEM (HIPS)		
1.	The solution shall be a purpose-built server security solution with all required server security modules.	
2.	The solution shall be based on client / server architecture. The clients shall be loaded on machines and the server shall distribute the definition and / or other updates to the clients on periodic basis and as and when required.	
3.	The Server security client should be available on the following Operating Systems Platforms: Windows Server 201X All versions, Redhat Enterprise Linux current available and supported versions.	
4.	The server security solution should have the following protection mechanism: Antivirus and antispyware, Host based Firewall, Host Intrusion prevention system, Application Change Control, File Integrity Monitoring.	
5.	The solution must protect against all kinds of viruses, Trojans and worms including but not limited to: boot sector, master boot sector, memory resident, macro, stealth and polymorphism etc.; and any other forms of exploits. The solution shall also protect against certain non-virus threats, such as Spyware, adware, dialers, joke programs, remote Access and hacking tools, which can be used with malicious intent. Ransomware protection to be available as part of the solution.	
6.	Solution shall inspect applications, as well as the applications' sub-components (DLLs) as they are executed. Solution shall have the ability to detect malicious applications that attempt to spawn themselves over the network.	
7.	After the detection of a malware infection, the solution should remove all the traces of malware from the system by cleaning up the following: Detect Malicious Files; Affected registry entries; Any new files dropped by malware; windows service created by malware;	
8.	The solution shall protect documents against unauthorized encryption or modification.	
9.	The solution shall protect against fileless malware.	
10.	The solution shall provide detection and blocking of Command and control (C&C) traffic.	
11.	The solution shall scan for malware on system start-up using the real-time scan.	
12.	The solution shall provide real time protection against malware. The solution shall scan when a file is received, opened, downloaded, copied, or modified to detect any security risks.	
13.	The solution shall allow for scheduling of a system scan on pre-defined frequency or time.	
14.	The solution shall allow the administrator to initiate a manual scan of the system.	

15.	The solution shall be able to add files, folders or extensions to an exclude list so that they are not scanned on access.	
16.	The solution shall support scanning of compressed file formats like ZIP, RAR etc.	
17.	The solution shall allow the user/administrator to initiate a scan on the memory as well as hard disk. The solution shall perform memory process scanning for detection of memory resident malware.	
18.	The solution shall provide protection against malicious and dangerous websites.	
19.	The solution shall monitor critical operating system and application elements such as directories, files, registry keys and values to detect and report suspicious activity such as modifications or changes in ownership/permissions.	
20.	The solution shall have the capability of restrict usage of unauthorized applications. The solution shall provide protection against execution of unknown and unwanted applications on the servers.	
21.	The solution shall allow monitoring & blocking of Inbound and Outbound traffic.	
22.	The Client Firewall should be able to allow or deny traffic from a specified port or range of ports and IP Addresses.	
23.	The solution shall protect the server against the exploitation of vulnerabilities in operating system and other applications.	
24.	The Solution should provide virtually patching (shielding) from exploitation attempts against known but unpatched vulnerabilities.	
25.	The solution should be able schedule the recommendation scan to add and remove new HIPS protection rules automatically.	
26.	The solution shall utilize pre-execution and runtime machine learning on Windows systems to detect malware, which do not have any signatures.	
27.	The solution shall utilize behavioral techniques on Windows systems to detect malware based on the behavior of the file.	
28.	The OEM should have a 24/7 security service update and should support real time signature update of the system as soon as updates are released.	
29.	The solution shall have an update server, which shall download the definitions/ updates and distribute them to the clients.	
30.	The solution shall be able to initiate virus scan on all machines remotely to scan all machines in case of an outbreak.	
31.	The solution should provide a single unified management dashboard to view the status of installed agents.	
32.	The solution shall offer enterprise-wide visibility over the status of all the deployed components from a central dashboard. The dashboard shall provide a summarized view to analyze top threats & summary of malware traffic or any other threats.	
33.	The solution shall offer creation of granular policies based on flexible attributes which can be deployed with consistent policy enforcement across distributed environments and multiple components from one management platform.	
34.	The solution shall offer a central repository of the updates and signatures/ definitions that can be distributed to the managed components.	
35.	The solution shall be able to receive logs from the managed components and endpoints and store them centrally.	
36.	The solution shall collect the events occurring on endpoints. The solution shall also provide the functionality to forward of these events to the SIEM.	

37.	The solution shall provide alerts to users in case of any security incident along with a course of action, in case of any failure to clean.	
38.	The solution must provide notifications for important events. The notifications must be send through multiple alerting mechanisms including email and SNMP traps.	
39.	The solution shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges for different components.	
40.	Solution should provide logging of administrative activities performed by the administrators.	
41.	The proposed solution should be capable of providing detailed reports containing data from all the deployed components. These shall include reports for policy violation, malware detected, traffic, users and groups etc.	
42.	The proposed solution should support scheduled report generation.	
43.	Exporting of reports to PDF or text format shall be available.	
44.	The proposed solution should integrate with the UIIC's Security Information & Event management (SIEM) - McAfee.	
45.	The bidder shall propose Support & Subscription / warranty services for 5 years from direct OEM for 24x7x365 with unlimited incident support including unlimited upgrades and updates.	

ANNEXURE 10 – Delivery Locations

Below are the delivery locations:

DC LOCATION:

UNITED INDIA INSURANCE COMPANY LIMITED
M/s. Sify Technologies Ltd - Airoli DC,
Reliable Plaza, Plat No-K10, Kalwa Block,
TTL Industrial Area, Thane,
Mumbai-400 708

DR LOCATION:

UNITED INDIA INSURANCE COMPANY LIMITED
Ctrls Datacenters Ltd.,
16, Software Units Layout, Madhapur (Hitech City),
Hyderabad, Telangana – 500 081.

Signature:

Name:

Designation:

ANNEXURE 11 – Pre Integrity Pact (Format)

(Bidders to submit 2 (two) copies of integrity pact in ₹ 100 stamp paper)
[To be included in 'Cover – A' Eligibility Bid Envelope]

RFP Ref. 000100/HO IT/RFP/734/2021-2022 - "Tender for Proposal (RFP) for SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"
Date:

1 General

This pre-bid-pre-contract Agreement (hereinafter called the Integrity Pact) is made at _____place _____on _____ day of the month of _____, 2019 between United India Insurance Company Limited, having its Head Office at 24, Whites Road, Chennai – 600 014 (hereinafter called the "BUYER/UIIC", which expression shall mean and include, unless the context otherwise requires, its successors and assigns) of the First Part and M/s._____represented by Shri./Smt._____, Chief Executive Officer (hereinafter called the "BIDDER/SELLER" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

WHEREAS the BUYER proposes to issue RFP for supply, installation and maintenance of firewall and the BIDDER/SELLER is willing to offer/has offered the services and WHEREAS the BIDDER is a private company/public company/Government undertaking/partnership/registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a corporation set up under an Act of Parliament.

NOW, THEREFORE,
To avoid all forms of corruption by following a system that is fair, transparent and free from any influence /prejudiced dealing prior to, during and subsequent to the currency of the contract to be entered into with a view to:

• Enabling the BUYER to obtain the desired said stores/equipment/services at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement and

• Enabling BIDDERs to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption in any form by its officials by following transparent procedures.

The parties hereto hereby agree to enter into this integrity Pact and agree as follows:

2 Commitments of the BUYER

2.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries, any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract

in exchange for an advantage in the bidding process, bid evaluation, contracting or implementation process related to the contract.

2.2 The BUYER will during the pre-contract stage, treat all BIDDERs alike, and will provide to all BIDDERs the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERs.

2.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2.4 In case any such preceding misconduct on the part of such official(s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facia found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by the BUYER and during such a period shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

3 Commitments of BIDDERs

The BIDDER commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post-contact stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any officials of the BUYER, connected directly or indirectly with bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.

3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe , gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavour to any person in relation to the contract or any other contract with the Government.

3.3 BIDDERs shall disclose the name and address of agents and representatives and Indian BIDDERs shall disclose their foreign principals or associates.

3.4 BIDDERs shall disclose the payments to be made by them to agents/brokers or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacture/integrator/authorized government sponsored export entity of the defence stores and has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, or has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of the BUYER or their family members, agents, brokers or any other intermediaries in connection with contract and the details of services agree upon for such payments.

3.7 The BIDDER will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation, contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 The BIDDER shall not use improperly, for purposes of competition or personal gain or pass on the others, any information provided by the BUYER as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11 The BIDDER shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

3.12 If the BIDDER or any employee of the BIDDER or any person acting on behalf of the BIDDER, either directly or indirectly, is a relative to any of the officers of the BUYER or alternatively, if any relative of the officer of the BUYER has financial interest/stake in the BIDDER's firm, the same shall be disclosed by the BIDDER at the time of filling of tender. The term 'relative' for this purpose would be as defined in Section 2 (77) of the Companies Act, 2013.

3.13 The BIDDER shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of the BUYER.

4 Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three years immediately before signing of this integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify BIDDER's exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender process or the contract, if already awarded, can be terminated for such reason.

5 Earnest Money (Security Deposit)

5.1 While submitting commercial bid, the BIDDER shall deposit an amount of ₹ 25,00,000/- (Rupees Twenty-Five lakhs only) as Earnest Money/Security Deposit, with the BUYER through any of the following instrument.

(i) in the form of electronic credit only to UIIC Bank Account.

(ii) A confirmed guarantee by an Indian Nationalised Bank, promising payment of the guaranteed sum to the BUYER immediately on demand without any demur Whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.

(iii) The Earnest Money/Security Deposit shall be valid for a period of 3 months OR the complete conclusion of the contractual obligation to the complete satisfaction of both the buyer and bidder, including the warranty period, whichever is later.

(iv) In case of the successful BIDDER a clause would also be incorporated in the Article pertaining to Performance Bond in the Purchase Contract that the provision of Sanctions for Violation shall be applicable for forfeiture of Performance Bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

(v) No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.

(vi) A confirmed guarantee by an Indian Nationalised Bank, promising payment of the guaranteed sum to the BUYER immediately on demand without any demur whatsoever and without seeking any reasons whatsoever. The demand for payment by the BUYER shall be treated as conclusive proof of payment.

6 Sanctions for Violations

6.1 Any breach of the aforesaid provision by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required:

I. To immediately call off the pre contract negations without assigning any reason or giving any compensation to the BIDDER. However, the proceedings with other BIDDER(s) would continue

II. The Earnest Money Deposit (in pre-contract stage) and /or Security Deposit/Performance Bond) (after the contract is signed) shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason therefore.

III. To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER

IV. To recover all sums already paid by the BUYER, and in case of Indian BIDDER with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a bidder from a country other than India with interest thereon at 2% higher than LIBOR. If any outstanding payment is due to the bidder from the buyer in connection with any other contract for any other stores, such outstanding payment could also be utilized to recover the aforesaid sum and interest.

V. To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the BIDDER, in order to recover the payments, already made by the BUYER along with interest.

VI. To cancel all or any other Contracts with the BIDDER, the BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/rescission and the BUYER shall be entitled to deduct the amount so payable from the money(s) due to the BIDDER

VII. To debar the BIDDER from participating in future bidding processes of the buyer or its associates or subsidiaries for minimum period of five years, which may be further extended at the discretion of the BUYER.

VIII. To recover all sums paid in violation of this Pact by BIDDER(s) to any middleman or agent or broker with a view to securing the contract.

IX. In cases where irrevocable Letters of Credit have been received in respect of any contract signed by the BUYER with BIDER, the same shall not be opened.

X. Forfeiture of Performance Bond in case of decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this Pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at para 6.1(i) to (x) of this Pact also on the commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defied in Chapter IX of the Indian Penal code, 1860 or Prevention of Corruption Act, 1988 or any other statute enacted for prevention of corruption.

7 The decision of the BUYER to the effect that a breach of the provision of this Pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the independent Monitor(s) appointed for the purposes of this Pact.

8 Fall Clause

8.1 The BIDDER undertakes that it shall not supply identical solution(s) in comparable business circumstances at a price lower than that offered in the present bid in respect of any other Public Sector Bank / Insurance Company in India and if it is found that within one year after the signing of contract that identical solution(s) is supplied by the BIDDER to any other Public Sector Bank / Insurance Company

in India at a lower price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

9 Independent Monitors

9.1 The BUYER is in the process of appointing Independent Monitors (hereinafter referred to as Monitors) for this Pact in consultation with the Central Vigilance Commission.
9.2 The task of the Monitors shall be to review independently and objectively, whether and to what extent the parties comply with the obligations under this Pact.
9.3 The Monitors shall not be subject to instruction by the representatives of the parties and perform their functions neutrally and independently.
9.4 Both the parties accept that the Monitors have the right to access all the documents relating to the project/procurement, including minutes of meetings.
9.5 As soon as the Monitor notices or has reason to believe, a violation of the Pact, he will so inform the Authority designated by the BUYER
9.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documents. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality
9.7 The BUYER will provide to the Monitor sufficient information about all meetings among the parties related to the Project provided such meetings could have an impact on the contractual relations between the parties. The parties will offer to the Monitor the option to participate in such meetings

9.8 The Monitor will submit a written report to the designed Authority of the BUYER within 8 to 10 weeks from the date of reference or intimation to him by the BUYER/BIDDER and should the occasion arise, submit proposals for correcting problematic situations.

Sri. A. Vijay Anand, IAS (Retd.)	**Sri. Joginder paul sharma, IAS (Retd.)**
303,1 salarpuria paradis, aggas abbas ali road, Ulsoor, Benagaluru 560 042	D-266, sector – 47, Noida, UP - 20130

10 Facilitation of Investigation

In case of any allegation of violation of any provision of this Pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

11 Law and Place of Jurisdiction

12 This Pact is subject to Indian Law. The place of performance and jurisdiction is the seat of the BUYER.

13 Other Legal Actions

The action stipulated in this integrity Pact are without prejudice to any other legal action that may follow in accordance with the provisions of the extant law in force relating to any civil or criminal proceedings.

14 Validity

14.1 The validity of this Integrity Pact shall be from date of its signing and extend upto 3 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/Seller, including warranty period, whichever is later in case BIDDER is unsuccessful, this integrity Pact shall expire after six months from the date of the signing of the contract.

14.2 Should one or several provisions of the Pact turn out to be invalid, the remainder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

15 The parties hereby sign this integrity Pact, at _____ on _____

(a) for & on behalf of United India Insurance Co. Ltd	(a) for & on behalf of (BIDDER'S NAME)
DEPUTY GENERAL MANAGER	**CHIEF EXECUTIVE OFFICER**
---	---
In the presence of:	In the presence of:
Witnesses - 1:	Witnesses - 1:
Witnesses - 2:	Witnesses - 2:

ANNEXURE 12 – Pre-Bid Query Format

Ref. 000100/HO IT/RFP/734/2021-2022 "REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

Date:

Dear Sir,

Subject: Queries w.r.t. Ref. 000100/HO IT/RFP/734/2021-2022 **for** "REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

S#	Page#	Point / Section	Existing Clause	Query
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

ANNEXURE 13 – Buy Back Infra

DC Site

S#	MAKE/SERVER IDENTITY	SERIAL NO/MT NO
1	IBM SAN SWITCH	TYPE:2498-B24
		S/N:10365DR
2	IBM STORAGE(CONTROLER)	V3700
		MT-207224C
		S/N:7844475
		P/N:2072S2C
2	IBM STORAGE (EXPANSION)	V3700
		MT-207224E
		S/N:7844846
		P/N:2072SEV
3	IBM X3650 M4	MT-7915 AC1
		S/N:06BXCVN
		PID:7915B2A
4	IBM X3650 M4	MT-7915 AC1
		S/N:06BXCVR
		PID:7915RXV
5	IBM X3650 M4	MT-7915 AC1
		S/N:06BXCVT
		PID:7915RXV
6	IBM X3650 M4	MT-7915 AC1
		S/N:06BXCVP
		PID:7915RXV
7	IBM SAN SWITCH	TYPE:2498-B24
		S/N:10365GA
8	IBM LIBRARY	MODEL:TS3200
		S/N:78K8597
		MT-3573(L4U)
9	IBM HMC PAENEL	S/N:7316TF4102256W
		P/N:00E2039
10	IBM HCM SERVER	X3550 M4
		S/N:7914PKYKQ2RR9
11	IBM POWER SERVER 710	MT-8231E1D
		S/N:214FDFV
		EID:000435
12	IBM POWER SERVER 710	MT-8231E1D
		S/N:214FDCV
		EID:000435

DR Site:

S#	MAKE/SERVER IDENTY	SERIAL NO/MT NO
1	IBM Tap Autoloader	TYPE:9572-S6H
		S/N-SIN68-15622
2	IBM X3650 M4	MT-7915 AC1
		S/N-06BXCVV
3	IBM X3650 M4	MT-7915 AC1
		S/N-06BXCVW
4	IBM POWER SERVER 710	MT-8231 E1D
		S/N-214FDDV
5	IBM STORAGE	V3700
		MT-2072 24C
		S/N-7844542
		P/N-2072S2C
6	IBM SAN SWITCH	TYPE:-2498-B24
		S/N:-10365-GY

Signature:

Name:

Designation:

ANNEXURE 14 – Land Border with India

< To be submitted in the Bidder's & OEM's letter head >

Ref. No:
To
The Deputy General Manager
Information Technology Department
United India Insurance Company Limited
Head Office, 19, 4th Lane, Nungambakkam High Road,
Chennai – 600034

Subject: Offer for RFP Ref. No. 000100/HO IT/RFP/734/2021-2022 "RFP for SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

Dear Sir/Madam,

I have read Office Memorandum F.No.6/18/2019-PPD dated 23.07.2020 issued by the Ministry of Finance, Department of Expenditure, Public Procurement Division inserting Rule 144 (xi) in GFRs 2017 which defines clauses regarding restrictions or procurement from a bidder of a country which shares a land border with India. I certify that _____(Bidder / OEM Name) is not from such a country or, if from such a country, has been registered with the competent authority, I certify that this bidder / OEM fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the competent authority shall be attached.]"

Authorized Signatory Name Designation Office Seal

Place:
Date:

Annexure 15: Hardware End of Life and Support Declaration

(To be submitted in the OEM's letterhead and should be signed by Authorized signatory of the OEM)

[To be included in 'Cover – A' Eligibility Bid Envelope]

Ref. 000100/HO IT/RFP/734/2021-2022

To
The Deputy General Manager
Information Technology Department
United India Insurance Co. Ltd.
Head Office NALANDA, # 19,4th Lane
Uthamar Gandhi Salai,
(Nungambakkam High Road)
Chennai – 600034

Re: Your RFP Ref. 000100/HO IT/RFP/194/2021-2022 – "REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, AND MAINTENANCE OF HARDWARE AND SUPPLIED SOFTWARE AT DC & DR TOWARDS UIIC CORPORATE MAILING SOLUTION"

Dear Sir/Madam,

We _____ (OEM & Address) has supplied _____ (Hardware Make / Model). We confirm that the Supplied hardware will not be end-of-life / End-of-sale during contract period and will be under support from the date of PO to next 7 years. The bug/Patches and release will be available to UIIC for above mentioned 7 years duration.

Name: _____

Designation: _____

Date: _____

Seal & Signature: _____

ANNEXURE 16 - Bid Submission Check List – For Bidders

S#	Document	Attached (Yes/No)	Page#
COVER A			
1	Tender Fee remittance details.		
2	Proof of Earnest Money Deposit (EMD) amount deposited in UIIC Account / Bank Guarantee for EMD as per Annexure 5.		
3	Pre-Contract Integrity Pact as per Annexure 11 in stamp paper (2 copies).		
4	Letter of Authorization as per Annexure 1.		
5	Eligibility Criteria Declaration Form as per Annexure 6. And supporting documents as detailed in Annexure 6.		
6	Authorization Form by Power of Attorney of OEM as per Annexure 3.		
7	Proof of Power of Attorney of the OEM.		
8	Authorized signatory of the Bidder signing the Bid Documents should be empowered to do so. Proof in the form of letter signed by a Director or Company Secretary to be attached.		
9	Statement of Nil deviation as per Annexure 4.		
10	No Blacklisting Declaration as per Annexure 2.		
11	Non-Disclosure Agreement as per Annexure 8		
13	Compliance of Annexure 16.		
14	Land border with India as per annexure 14.		
15	Hardware EOL/ EOS as per Annexure 15.		
COVER B:			
1	Compliance Statement for the prescribed Technical specifications as per annexure. Along with all supporting documents as detailed in Annexure 9.		
2	Technical Documentations (if any)		
COVER C:			
1	Commercial Bid as per Annexure 7		

INSTRUCTION TO BIDDERS FOR ONLINE SUBMISSION

The bidders are required to submit soft copies of their bid electronically on the e-Nivida Portal using valid Digital Signature Certificates. Below mentioned instructions are meant to guide the bidders for registration on the e-Nivida Portal, prepare their bids in accordance with the requirements and submit their bids online on the e-Nivida Portal. For more information bidders may visit the UIIC e-Nivida Portal (https://uiic.enivida.com/).

1. REGISTRATION PROCESS ON ONLINE PORTAL

a) Bidders to enrol on the e-Procurement module of the portal https://uiic.enivida.com/ by clicking on the link **"Bidder Enrolment".**
b) The bidders to choose a unique username and assign a password for their accounts. Bidders are advised to register their valid email address and mobile numbers as part of the registration process. This would be used for any communication from the e-Nivida Portal.
c) Bidders to register upon enrolment, with their valid Digital Signature Certificate (Class III Certificates with signing and Encryption key) issued by any Certifying Authority recognized by CCA India with their profile.
d) Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSCs to others which may lead to misuse.
e) Bidder then logs in to the site through the secured log-in by entering their user ID/password and the password of the DSC / e-Token.

2. TENDER DOCUMENTS SEARCH

a) Various built-in options are available in the e-Nivida Portal like Department name, Tender category, estimated value, Date, other keywords, etc. to search for a tender published on the Online Portal.
b) Once the bidders have selected the tenders they are interested in, they may download the required documents/tender schedules. These tenders can be moved to the respective 'Interested tenders' folder.
c) The bidder should make a note of the unique Tender No assigned to each tender; in case they want to obtain any clarification/help from the Helpdesk.

3. BID PREPARATION

a) Bidder should take into account any corrigendum published on the tender document before submitting their bids.
b) Please go through the tender advertisement and the tender document carefully to understand the documents required to be submitted as part of the bid.
c) Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that needs to be submitted. Any deviations from these may lead to rejection of the bid.
d) Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document/schedule and generally, they can be in PDF/XLSX/PNG, etc. formats.

4. BID SUBMISSION

a) Bidder to log into the site well in advance for bid submission so that he/she uploads the bid in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
b) The bidder to digitally sign and upload the required bid documents one by one as indicated in the tender document.

c) Bidders to note that they should necessarily submit their financial bids in the prescribed format given by department and no other format is acceptable.
d) The server time (which is displayed on the bidders' dashboard) will be considered as the standard time for referencing the deadlines for submission of the bids by the bidders, the opening of bids, etc. The bidders should follow this time during bid submission.
e) All the documents being submitted by the bidders would be encrypted using PKI encryption techniques to ensure the secrecy of the data, which cannot be viewed by unauthorized persons until the time of bid opening.
f) The uploaded tender documents become readable only after the tender opening by the authorized bid openers.
g) Upon the successful and timely submission of bids, the portal will give a successful bid submission message & a bid summary will be displayed with the bid no. and the date & time of submission of the bid with all other relevant details.
h) The off-line tender shall not be accepted and no request in this regard will be entertained whatsoever.

5. AMENDMENT OF BID DOCUMENT

At any time prior to the deadline for submission of proposals, the department reserve the right to add/modify/delete any portion of this document by the issuance of a Corrigendum, which would be published on the website and will also be made available to the all the Bidder who has been issued the tender document. The Corrigendum shall be binding on all bidders and will form part of the bid documents.

6. ASSISTANCE TO BIDDERS

a) Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender.
b) Any queries relating to the process of online bid submission or queries relating to e-Nivida Portal, in general, may be directed to the 24x7 e-Nivida Helpdesk. The contact number for the helpdesk is **Gagan (8448288987/89/eprochelpdesk.01@gmail.com), Ambika (8448288988/94/eprochelpdesk.02@gmail.com), Retnajith (9355030607), Sanjeet (8882495599), Rahul Singh (8448288982), Amit (9355030624), Abhishek Kumar (9355030617), Tariq (9355030608)**

7. The tender inviting authority has the right to cancel this e-tender or extend the due date of receipt of the bid(s).
8. The bid should be submitted through e-Nivida portal (https://uiic.enivida.com/) only.

END OF RFP