REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, IMPLEMENTATION, INTEGRATION, MAINTENANCE AND SUPPORT OF SECURITY SYSTEM

000100/HO IT/RFP/138/2020-21

UNITED INDIA INSURANCE CO. LTD

INFORMATION TECHNOLOGY DEPARTMENT

NALANDA

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 scope of work for the Bidder for Request for Proposal for Supply, Installation, Implementation, Integration, Maintenance and Support of Security System.

M/s. Sify Technologies Ltd. & M/s. NTT who are currently acting as NOC service providers in UIIC are not allowed to participate in this current RFP.

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.

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
ATR	Acceptance Test Report
ATS	Annual Technical Support
CVC	Central Vigilance Commission
HO	Head Office
RO	Regional Office
DO / BO	Divisional Office / Branch Office
DC	Data Center
DR	Disaster Recovery

INR	Indian Rupees
IP	Internet Protocol
IT	Information Technology
ISP	Internet Service Provider
LAN	Local Area Network
Mbps	Mega Bits per Second
MPLS	Multi-Protocol Label Switching
RF	Radio Frequency
EMS	Event Monitoring System
NMS	Network Management System
BCP	Business Continuity Planning
PO	Purchase Order
OS	Operating System
TO	Technical Offer
ToR	Terms of Reference
UAT	User Acceptance Test
SME	Subject Matter Expert
SIEM	Security Information and Event Management
PIM	Privilege Identity Management
DdoS	Distributed Denial of Services
WAF	Web Application Firewall
DAM	Database Activity Monitoring
AD	Active Directory
BFSI	Banking, Financial Services and Insurance

1. BID SCHEDULE AND ADDRESS

S.No.	Description	
1.	Name of the Tender	RFP for Supply, Installation, Implementation, Integration, Maintenance and Support of Security System
2.	Tender Reference Number	000100/HO IT/RFP/138/2020-21 DATED. 13.08.2020
3.	Tender Release Date	21.08.2020
4.	Last date for queries through email (rfp.networks@uiic.co.in)	31.08.2020
5.	Pre-bid meeting	04.09.2020 (03.00 PM via Video Conferencing)
6.	Last date for bid submission	18.09.2020 (03:00 PM)
7.	Online Bid Submission @	https://uiic.enivida.com/
8.	Tender Fee (Non-Refundable)	₹ 10,000 /-(Rupees Ten Thousand only)
9.	EMD Fee	₹ 50,00,000/-(Rupees Fifty Lakh only)
10.	Email ID for communication	rfp.networks@uiic.co.in

Note:

Bids will be opened in the virtual presence of the Bidders' representatives who opts to attend through Video Conferencing that will be facilitated by UIIC.

Pre-bid meeting will also be held via Video Conferencing, since physical gathering may not be feasible considering the present pandemic situation due to COVID-19.

To attend pre-bid meeting through Video Conferencing:

Those bidders who desire to attend pre-bid meeting through 'Video Conferencing' are requested to send their names along with email-ID & mobile number to rfp.networks@uiic.co.in at least two days prior to date of Pre-bid meeting along with the payment details of the tender fee (This would ease the process of sharing VC link for the meeting). A maximum of two persons would be allowed for each bidder to attend the Video Conferencing.

After our replies to pre-bid queries raised by the vendors are published, another round of pre-bid meeting may be conducted on 15.09.2020 to discuss about clarifications/clearing doubts on our published replies for pre-bid queries, if any.

To attend 'Bid opening' meeting through Video Conferencing:

Those bidders who desire to attend the meeting through 'Video Conferencing' are requested to send their names along with email-ID & mobile number to rfp.networks@uiic.co.in at least two days prior to date of bid submission date along with the payment details of the tender fee (This would ease the process of sharing VC link for the meeting). A maximum of two persons would be allowed for each bidder to attend the Video Conferencing.

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, Implementation, Integration, Maintenance and Support of Security System for a period of five years (Extendable for one year on mutually agreed terms and conditions). 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 SP 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 SP 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 FOR BIDDERs/OEMs

S.No.	Eligibility Criteria	Documentary Proof Required	Bidder/OEM
a.	The Bidder should be a Registered Company in India under the 'Companies Act' and should be in existence in India for a minimum of five (05) years as on 31.03.2020.	Copy of the Certificate of Incorporation issued by Registrar of Companies.	Bidder
b.	The Bidder should be ISO 9000/9001, ISO 20000 and ISO/IEC 27001 certification holder company,	Photocopies of the certificates to be	Bidder

	with certifications valid at the time of bid submission.	provided.	
c.	The bidder should have an average annual financial turnover of at least ₹ 200 Crore for the last three financial years viz. 2017-18, 2018-19 and 2019-20.	Audited financial statements / Certificate from Auditor	Bidder
d.	The bidder should have made Net Profit (Profit After Tax – PAT) after taxation in any of the last three financial years viz. 2017-18, 2018-19 and 2019-20.	Audited financial statements / Certificate from Auditor	Bidder
e.	The bidder should not have been blacklisted/debarred by any Government Department, Agencies or Public Sector Undertakings in India as on the date of submission of the tender.	As per ANNEXURE 2	Bidder
f.	The Bidder should have implemented or have under implementation, minimum 3 of the below mentioned security solutions for atleast 1 BFSI Customer in India with minimum 1000 offices/Branches i.PIM ii.SIEM iii.DDoS iv.WAF v.DAM	Successful completion certificates or Credential Letters Or Copy of Contract / Purchase order from the Client for implemented projects Or Copy of Contract / Purchase order for under implementation projects	Bidder
g.	Bidder should be providing SIEM Solution to minimum 2 BFSI customers in India	Purchase order copy / Project Sign off document /Client Certificate should be attached as proof.	Bidder
h.	The bidder must have minimum five (5) IT Security professionals on their payroll with certification in CISA / CISSP / CISM / CEH / CCSA.	Self-Declaration/ Undertaking to this effect to be submitted by the bidder	Bidder

i.	The Bidder must warrant that key project personnel to be deployed in this project should have managed a similar project (SIEM/DAM/DDoS/PIM/WAF) in the past.	Self-Declaration/ Undertaking to this effect to be submitted by the bidder and Details of the personnel indicating their qualifications, professional experience and projects handled.	Bidder
j.	Bidder should be either Original Equipment Manufacturer (OEM) of Security devices/software solutions or authorized partner of OEM. In case the bidder is an Authorized partner of the OEM, Bidder must submit the authorization letter from each of the OEM for the solutions proposed.	Authorization letter on OEM's letterhead as per ANNEXURE 3.	Bidder/OEM
k.	Each of the proposed OEM solution mentioned below should have been implemented and running in at least 2 BFSI customers with more than 1000 branches each in India not necessarily by the same bidder. 1. SIEM 2. PIM 3. DAM 4. WAF 5. DDoS	Purchase order copy / Project Sign off document / Client Certificate should be attached as proof.	OEM

Note:

i. Bidders need to ensure compliance to all the eligibility criteria points
ii. M/s. Sify Technologies Ltd. & M/s. NTT who are currently acting as NOC service providers in UIIC are not allowed to participate in this current RFP.
iii. Public Sector / scheduled commercial banks do not include regional rural banks and cooperative banks.
iv. In-case of corporate restructuring, the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
v. 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.
vi. While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I) 2 / 161730 dated 13.01.2012): 'Commission has decided that in all cases of procurement, the following guidelines may be followed:

a. In an RFP, either the Indian agent on behalf of the Principal/OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.
b. If an agent submits bid on behalf of the Principal/OEM, the same agent shall not submit a bid on behalf of another Principal/OEM in the same RFP for the same item/product.'

2.5 ELIGIBILITY BID DOCUMENTS

i. Compliance to Eligibility Criteria as per RFP Section 2.4 along with all relevant supporting documents
ii. Application Form for Eligibility Bid as per ANNEXURE 6.
iii. EMD of Rs.50,00,000 (Rs. Fifty Lakhs only) (Exempt for eligible entities (i.e. MSME/NSIC), as per Government of India Guidelines, subject to submission of the relevant certificate. Certificate shall be valid on the date of Bid Submission) in the form of BG favoring 'The United India Insurance Co. Ltd.' as per ANNEXURE 5.
iv. The corporate profile of the bidder (printed corporate brochure is preferred).
v. The profile of the bidder (as per ANNEXURE 6)
vi. List of bidder's support/service locations in India.
vii. Bidder shall submit PAN number, GSTIN.
viii. Undertaking that the Bidder has quoted for all items and the bid validity will be for 180 days from the date of submission of bid.
ix. The power of attorney or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the Bidder
x. The power of attorney or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the OEM
xi. Statement of Nil Deviations (ANNEXURE 4)
xii. Pre Integrity Pact (ANNEXURE 13 on Stamp Paper)

2.6 TECHNICAL BID DOCUMENTS

i. Executive Summary of Bidder's response. The Executive Summary should be limited to a maximum of five pages and should summarize the content of the response. The Executive Summary should initially provide an overview of Bidder's organization and position with regards to proposed solution and professional services. A summary of the Bidder's products and services that will be provided as a part of this procurement should follow.
ii. Detailed technical note covering the detailed scope of work.
iii. Compliance to Minimum Functional and Technical Specifications as per ANNEXURE 10.
iv. The Bidder should also include a replica of the masked final commercial bid without prices in the technical bid. The Bidder must note that the masked commercial bid should be actual copy of the commercial bid submitted with prices masked and not copy of the Pro-forma/format of the ANNEXURE 7 – Commercial bid format in the RFP. The Masked Bill of Material shall include details of the Software (Name, Version Details, License Metrics etc.), Hardware (Name of the Equipment with OEM Make and Model, CPU, RAM, HDD, Cores etc.), Facility Management (Efforts of Bidder and OEM's) etc.
v. Implementation plan & warranty support

vi. Support Plan
vii. User Training Plan
viii. Transition Plan

Note:

i. Participation in this tender will mean that the Bidder has accepted all terms and conditions and clauses of this tender and subsequent modifications to this tender, if any.
ii. The documentary evidence sought in respect of the eligibility criteria would be essential. Bids not accompanied by documentary evidence may be subject to rejection. Clarification/Additional documents, if any, sought by UIIC from the Bidder has to be submitted within the stipulated time. Otherwise, bid will be rejected and no further correspondence in the matter will be entertained by UIIC.
iii. Any alterations, erasures or discrepancies in figures etc. may render the bid invalid. The bid may be rejected in case of non-adherence to any of the instructions given above.
iv. UIIC reserves the right not to allow/permit changes in the technical specifications and not to evaluate the offer in case of non-submission or partial submission of technical details.
v. UIIC may at its discretion waive any minor non-conformity in any offer and the same shall be binding on all Bidders and UIIC reserves the right for such waivers.
vi. If UIIC is not satisfied with the technical specifications in any tender and observes major deviations, the technical bids of such Bidders will not be short-listed and the price bids of such Bidders will not be opened. No further discussions shall be entertained with such Bidders in respect of the subject technical bid.

2.7 COMMERCIAL BID DOCUMENTS

Commercial Bid documents should contain ANNEXURE 7 – Commercial bid format. The Commercial Bid should give all relevant price information and should not contradict the Pre-qualification and Technical Bid in any manner.
There should be no hidden costs for items quoted. The rates quoted should be in Indian rupees only and same should be rounded off to the nearest rupee and filled in both words and figures.

Evaluation Criteria

The competitive bids shall be submitted in three stages:

- Stage 1 - Eligibility Evaluation
- Stage 2 - Technical Evaluation
- Stage 3 - Commercial Evaluation

3. SCOPE OF WORK

3.1 SCOPE OF WORK - OVERVIEW

Cyber security has become a major concern over the past few years as hackers have penetrated the IT infrastructure of the enterprises with increasing frequency and sophistication. The protection of information infrastructure and preservation of the confidentiality, integrity and availability of information in cyberspace is the essence of a secure cyber space.

UIIC intends to procure the security solutions to enhance the security landscape of UIIC. The Scope includes procurement, installation, implementation, integration, maintenance and support of the solutions with all the relevant applications and infrastructure during the contract period. The objectives of the security solutions are as below.

The intent for Services / Solutions is covered in the below functional principles:

- **Prevention & Identification of Information Security Vulnerabilities**: The services/ solutions should be able to identify information security vulnerabilities in UIIC environment and prevent these vulnerabilities
- **Incident Management**: Reporting of information security incidents using appropriate tools. Track and monitor the closure of these information security incidents and escalation of these incidents to appropriate teams/ individuals in UIIC
- **Continuous Improvement**: Continuously improve services/ solutions as per the requirements from UIIC.

Based on the above principles, UIIC has envisaged the following security solutions, required over and above their current existing set of solutions to enhance the robust monitoring that are compliant with **ISO 27001, ISO 22301, IT Act 2000, Cyber Law, OWASP etc.**

a. Privilege Identity Management (PIM)
b. Security Information & Event Management (SIEM)
c. Distributed Denial of Service (DDoS)
d. Web Application Firewall (WAF)
e. Database Activity Monitoring (DAM)
f. Active Directory Migration

The Following are the brief activities bidder need to perform in order to successfully provide Supply, Installation, Implementation, Integration, Maintenance and Support of Security System:

i. Bidder need to define in consultation with UIIC different processes, policies, resources, technology, and interfaces.
ii. Bidder should conduct comprehensive business requirement mapping session with UIIC to understand their critical information/assets.
iii. Bidder must conduct policy identification exercise for target scope; perform asset classification based on understanding of business flow of critical data and business impacting processes. Bidder must provide adequate resources for implementation and facility management.
iv. During implementation OEM involvement should be spanning across all phases of implementation including Project Preparation, Solution Design Phase (Including Review/design of all the Policy Documents, Blueprints and other Solution documents), Configuration and Customization, Integration, Acceptance and Training. Post Implementation half yearly on-site review of the implementation and adequate support is required from the OEM. OEM is required to submit the review report directly to UIIC and bidder needs to close the same. OEM is required to provide the undertaking for the same.
v. Bidder must ensure that the end to end installation, configuration, parameterization, customization, implementation, integration, support and maintenance of all the solutions at central site i.e. DC & DR and branches/offices is to be carried out as per the UIIC Policies.
vi. Bidder must ensure procurement of the necessary solutions and the corresponding hardware,

software, database etc. required for implementing the proposed solutions.

vii. Bidder should take complete ownership to deploy the solutions seamlessly in existing infrastructure, if any upgrade/Update or replacement is needed in existing infrastructure, the same has to be informed to UIIC during the requirement gathering stage by bidder to deploy the solution with proper documentation.

viii. Bidder is required to work with the existing System Integrator(s) of the UIIC to integrate the security solutions with existing application platforms, server and storage environment, enterprise network, existing ISP, EMS/ NMS solutions, security solutions, ticketing tools etc.

ix. Bidder is required to provide the necessary personnel to manage the operations for the solutions in scope and to ensure SLA compliance.

x. UIIC reserves the right not to procure/implement any or all the proposed tools mentioned in this RFP. In such cases, only the cost for tools procured and/or implemented would only be payable to the bidder on pro-rata basis.

xi. UIIC will provide the network bandwidth for the in-scope solution. However, bidder is required to study the existing bandwidth at UIIC Premises and then need to suggest UIIC with the bandwidth requirement for in - scope solution, if any upgrade is required in terms of bandwidth bidder is required to provide UIIC with necessary documentation and support in order to upgrade the bandwidth (if required, UIIC will upgrade the Bandwidth post review of the submitted documents and bidder is not required to factor in any cost for upgrade of bandwidth). It is expected that the proposed solution to consume minimal bandwidth, so that it should not impact UIIC day to day business operations.

xii. UIIC will provide the required Ethernet switch ports. However, bidder is required to mention the number of Ethernet switch ports required for in- scope solution.

xiii. Bidder should bring all the tools and equipment (Including Fiber Cable and copper cables) for successful commissioning of hardware and software for successful implementation of Solution.

xiv. Bidder should be responsible for performing all the adequate cabling activity related to server, storage, appliances, SAN, LAN etc. at UIIC locations for successful commissioning of hardware and software. UIIC Data Center and Disaster Recovery Center runs on Fiber Channel/(Copper Channel).

xv. The bidder shall provide the detailed technical architecture comprising of hardware (including configuration) with operating systems and other application software in their technical bid.

xvi. The bidder shall be responsible for generation and submission of necessary documents required during various phases of project viz. planning, installation, commissioning, rollout, acceptance testing, project diagrams, LLD, HLD and other documents/reports etc. All such documents shall be considered only after the same is approved by UIIC.

xvii. Bidder to provide regular updates/upgrades/patches released by the OEM during the entire contract period and shall document and provide the documents to UIIC detailing all the changes in the solution and/or hardware. If required, bidder is required to provide the training to UIIC Officials of all the changes made in the solution at no additional cost to UIIC during the contract period.

xviii. All updates/upgrades/patches have to be applied in the UAT Environment within 15 days of release of updates/upgrades/patches by the OEM and approved by UIIC. Updates/upgrades/patches has to be applied in Production, within 30 days of release of updates/upgrades/patches by the OEM and approved by UIIC. However, there may be a requirement of deployment of critical patches on urgent basis, bidder to deploy the same post approval and as per the instructions from UIIC.

xix. Activities, specifications and Scope Mentioned in ANNEXURE 10 - Technical and Functional

Specification and ANNEXURE 9 - Volumetric also forms the part of the Scope of Work.

xx. All the services/solutions offered should be modular, scalable, and should be able to meet UIIC requirements during the period of contract.

xxi. All the services/solutions in scope needs to be designed and implemented with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime as outlined in this RFP.

xxii. It should be ensured that neither during installation nor during operations of the security solutions any of the existing infrastructure/business of UIIC is impacted.

xxiii. All the proposed security equipment/devices should be IPv6 compliant from Day 1.

xxiv. Bidder is required to adhere to Service Level Agreements (SLA), periodic monitoring and reporting requirement stated in the RFP and shall submit the report to UIIC for the same.

xxv. Continual improvement of the Security Operations as defined in the SLA.

xxvi. The solutions deployed should be modular, scalable and should be able to address UIIC requirements during the entire contract period, with the deployed hardware.

xxvii. The solutions and services in scope should be designed with adequate redundancy and fault tolerance to ensure compliance with SLAs for uptime as outlined in this RFP.

xxviii. Bidder should ensure dual power supply for all proposed hardware/appliances.

xxix. Bidder will be solely responsible for implementing and commissioning the solution (including software, hardware and required components) at DC, DR and all the offices in order to successfully implement and commission the proposed solutions.

xxx. Bidder is required to right size requirement (hardware and software). In case of any shortfall, bidder will provide additional hardware & software in order to meet the requirement at no additional cost to UIIC.

xxxi. The responsibility of integration of all the proposed solutions in this contract procured by UIIC lies with the bidder selected through this RFP. The UIIC shall provide adequate support to bidder for the purpose of integration.

xxxii. UIIC will not take any responsibility of any assumptions made by the bidder. It is the responsibility of the bidder to ensure successful implementation of the proposed solution. The bidder is also responsible for the accuracy of the bid and UIIC is not liable for any errors or assumptions made by the bidder.

xxxiii. All trainings will be arranged by the selected Bidder/OEM in UIIC's premise. UIIC will provide training room along with required no. of PCs and projector. Rest all expenses required for providing the training will be borne by Bidder.

xxxiv. The proposal submitted by the bidder should be a Nil Deviation Bid, any assumption, deviation or conditions quoted by the bidder anywhere in the proposal stands null & void.

xxxv. **Training:**

a. **Post Implementation:** Provide training to the UIIC personnel on operations, alert monitoring, policy configuration, generation of reports, and analysis of the reports, troubleshooting and familiarization of features and functionalities for all solutions independently.

b. The Bidder shall provide comprehensive training manual and other training documentation for all trainings. The training material should be mandatorily in English.

c. The Bidder may utilize the OEM resources in case the Bidder does not have adequately experienced resources for providing training.

d. The bidder will have to ensure that training is imparted in a professional manner through qualified personnel's and Course materials would have to be provided for the

same.

3.2 DETAILED SCOPE OF WORK

For the solutions in scope, the bidder is required to propose appliance, Hardware or software or a combination of hardware and software to meet the individual requirements put forward by UIIC for the respective solutions. Bidder is required to design, size, supply, install, commission and maintain the required security solutions for the period of contract.

3.2.1 IMPLEMENTATION & INTEGRATION

i. Implementation of the specified solutions and necessary hardware as per the technical requirement specified in the RFP is the responsibility of the bidder. Selected Bidder to ensure that the proposed solution (hardware and software) complies with all the functional and technical requirements as provided in ANNEXURE 10 - Technical and Functional Requirements & ANNEXURE 9 - Volumetric.
ii. Atleast 15 days before delivery of the solutions, the bidder is required to review the UIIC environment and specify any additional requirements that UIIC may need to provide for the implementation of the solution
iii. The bidder should provide the architecture for implementing the security solution on existing and any new network, which UIIC may procure during the contract period. It would be responsibility of the bidder to co-ordinate with the UIIC existing or any new Network Service Provider to ensure the proposed Security solutions is properly tested and made to work in UIIC environment.
iv. Bidder is required to integrate all the proposed tools and/or solutions with the UIIC provided ticketing tools in order to log tickets.
v. The Bidder to ensure that the security solutions and their operations comply with UIIC's information security policies and industry leading standards (such as ISO 27001, ISO 22301, IRDA, IT Act 2000, Cyber Law, etc.) and any applicable laws and regulations
vi. In addition, the bidder is responsible for impact assessment and modification of solution operations at no extra cost, on account of any changes to applicable information security policies/ procedures / standards/ regulations/any GOI Guidelines.
vii. Integrate the following with SIEM solution to provide a single view of events generated at no additional cost to UIIC during the contract period.
    a. Proposed Solution and hardware
    b. Existing Applications and Hardware
    c. New Applications and hardware to be implemented during the contract period
    d. Existing and New Devices
viii. OEM needs to validate all the documents submitted by the bidder during the implementation till the Go-Live of the respective solutions and bidder to submit the validation confirmation from the OEMs.
ix. Any interfaces required with existing applications/ infrastructure and new applications/ infrastructure for successful implementation and operations of the proposed solution (Hardware & Software) is in the scope of the bidder and should be developed by the bidder. UIIC Existing vendor will facilitate in integration of existing applications/infrastructure with the proposed Solution (Hardware & Software) however the prime responsibility of integration lies with the bidder.
x. Bidder is responsible for developing and implementing the security configuration, hardening of all the devices and software that are procured for Security Operations. Also, they must periodically

review the guidelines and configure.

xi. Post implementation, the bidder is responsible for integrating any additional logs that the UIIC may wish to monitor with the SIEM solution at no additional cost to the UIIC. Logs needs to be integrated with the SIEM solution through automated or manual mode. Bidder is required to provide the feasibility for both the modes of integration in coordination with the existing vendors. (Automated integration in the clause refers to the automated flow of logs from the source applications/ infrastructure to proposed SIEM)

xii. The major and primary responsibility of integration of solution with SIEM lies with the bidder selected through this RFP.

xiii. The bidder should note that the production, DR and non-production environment should be physically separate. Bidder can propose Logical separation/Virtualization within the Production, Non-Production and DR Environment.

xiv. Development and implementation of processes for management and operation including (but not limited to) the following processes:
    a. Configuration and Change Management
    b. Incident and Escalation management processes
    c. Daily standard operating procedures
    d. Training procedures and material
    e. Reporting metrics and continuous improvement procedures
    f. Data retention and disposal procedures
    g. BCP and DR plan and procedures for Security Solutions
    h. Security Patch management procedure

xv. Implement necessary security measures for ensuring the information security of the proposed Solutions.

xvi. The technical bid should include an overview of the processes mentioned above.
    a. Develop Escalation Matrix in order to handle Information Security Incidents efficiently.
    b. Provide necessary documentation for the operation, integration, customization, and training of each of the solutions in scope.

xvii. During Implementation Phase, bidder should propose at least one –Dedicated Project Manager - 100% Onsite Deployment (at Head Office), One - Solution Architect- Onsite Support to Project team on need basis, One - Security Expert- Onsite Support to Project team on need basis.

xviii. Bidder is required to prepare High Level Design Documents, Low Level Design Document, SRS, SOPs, Rules Document and configuration etc. in conjunction with UIIC Officials.

xix. Deployment Mode (Standalone/HA) for various solutions to be proposed is mentioned in the ANNEXURE 9 - Volumetric along with the required volumetric, bidder to propose the solution complying the requirements stated in ANNEXURE 10 - Technical and Functional Requirement and ANNEXURE 9 - Volumetric.

3.2.2 MEASURE & MANAGE FUNCTION

i. Measure & Manage Services must be provided for the tenure of the contract post successful Go-Live of security solutions.

ii. In case the resource goes on leave / absent/being replaced, UIIC should be intimated prior and suitable replacements/backup should be arranged by the bidder to ensure that regular functioning of the offices/locations does not get hampered. Bidder must provide the resumes of new resource, UIIC may interview the proposed resource and confirm their acceptability. In any event if a resource is found unfit

by UIIC, bidder shall agree to change the same and provide UIIC with a replacement within reasonable time to not affect the services/project timelines.

iii. **Manage Services Resources** should have at least 3 years of relevant experience in providing the Operation & Maintenance Services for Security solutions.

iv. **Project Manager** proposed should have at least 7 years of relevant experience in program managing any 3 of the below mentioned solutions:
- PIM
- SIEM
- DDoS
- WAF
- DAM
- Active Directory Migration

v. Project Manager/Support Executive has to support UIIC on 24X7 basis over phone/remote access whenever UIIC requests to make Policy/Rules changes and other demands in the Security Solutions, based on business requirement and on emergency basis

vi. Bidder will operate and maintain all the components of the Security Solutions (Software and Hardware) supplied through this RFP for the entire contract period. During Warranty and Maintenance phase, bidder shall ensure that service levels are monitored on continuous basis; service levels are met and are reported to UIIC.

vii. The bidder is required to establish the helpdesk and provide facilities management services to support the UIIC officials in performing their day-to-day functions related to the provided system. The Bidder shall setup a central helpdesk dedicated (i.e. on premise) for the Project implemented. This helpdesk would be Operational upon implementation of the Project and/or any solution. Bidder shall deploy manpower during Implementation, Warranty and Maintenance phases. The deployed resource shall report to UIIC's Project In-charge and work closely with Program Management Office of the project. Bidder may deploy additional resources based on the need of the project and to meet the defined SLAs.

viii. Helpdesk with 24x7 support shall be deployed, who shall be responsible for handling calls related to queries, fault, reporting, operations, trouble ticketing etc. Each of these agent's system will be provided space, phone and a desktop for receiving incoming calls from users and answer their queries. Provide 24x7 OEM support for the equipment and software components supplied as part of this tender.

ix. Bidder shall address all the errors/bugs/gaps in the functionality in the solution implemented (vis-à-vis the FRS, BRS and SRS signed off) at no additional cost during the Warranty and Maintenance phase.

x. All patches and upgrades (in Version) from OEMs shall be implemented by the Bidder ensuring customization done in the solution as per the UIIC's requirements are applied. Technical upgrade of the installation to the new version, as and when required, shall be done by the Bidder. Any version upgrade (in Version) of the software / tool / appliance by Bidder to be done after taking prior approval of UIIC and after submitting impact assessment of such upgrade at no additional cost to UIIC.

xi. Any changes/upgrades (in Version) to the software performed during the support phase shall subject to the comprehensive and integrated testing by the Bidder to ensure that the changes implemented in the system meets the specified requirements and doesn't impact any other function of the system. Release management for application software will also require UIIC approval. A detailed process in this regard will be finalized by Bidder in consultation with UIIC.

xii. Issue log for the errors and bugs identified in the solution and any change done in the solution shall be maintained by the bidder and should be periodically submitted to the UIIC team.

xiii. Bidder, at least on a monthly basis, will inform UIIC about any new updates/upgrades available for all software components of the solution along with a detailed action report. In case of critical security patches/alerts, the bidder shall inform about the same immediately along with his recommendations. The

report shall contain bidder's recommendations on update/upgrade, benefits, impact analysis etc. The bidder shall need to execute updates/upgrades though formal change management process and update all documentations and Knowledge databases etc. For updates and upgrades, Bidder will carry it out at no additional cost to UIIC by following defined process.

a. Errors and bugs that persist for a long time, impact a wider range of users and is difficult to resolve becomes a problem. Bidder shall identify and resolve all the problems in the identified solution (e.g. system malfunctions, performance problems and data corruption etc.).

b. Monthly report on problem identified and resolved would be submitted to UIIC team along with the recommended resolution.

xiv. All planned or emergency changes to any component of the system shall be through the approved Change Management process. The Bidder needs to follow all such processes (based on industry ITSM framework). For any change, Bidder shall ensure:

a. Detailed impact analysis
b. Change plan with Roll back plans
c. Appropriate communication on change required has taken place
d. Proper approvals have been received
e. Schedules have been adjusted to minimize impact on the production environment
f. All associated documentations are updated post stabilization of the change
g. Version control maintained for software changes. The bidder shall define the Software Change Management and Version control process. For any changes to the solution, Bidder must prepare detailed documentation including proposed changes, impact to the system in terms of functional outcomes/additional features added to the system etc. Bidder shall ensure that software and hardware version control is done for entire duration of Bidder's contract.

xv. Bidder shall maintain version control and configuration information for application software and any system documentation.

xvi. Bidder shall maintain at least the following minimum documents with respect:

a. The Bidder shall perform an in-depth analysis of the existing system and shall submit a detailed plan for the implementation of this project, including but not limited to the following:
    - Project Plan detailing each task with target date and assigned resource persons and installation of all supplied items and integration with existing infrastructure at DC, DR and UIIC Offices.
    - Architecture Diagram
b. Bidder shall submit this document to UIIC for review and any suggestions by UIIC will be incorporated therein.
c. High level design of whole system
d. Low Level design for whole system / Module level design
e. System requirements Specifications (SRS)
f. Any other explanatory notes about system, bidder shall also ensure updating of documentation of software system ensuring that:

i. User manuals and training manuals are updated to reflect on-going changes/enhancements.
ii. All the technical documents (HLD, LLD, Design Document, SRS, Implementation Plan, Rules & Policy documents etc.) submitted should be vetted by OEM's of respective components and bidder need to submit the OEM confirmation along with the documents.
iii. Bidder should ensure that all the required documentation is made available to UIIC. HLD, Project Plan etc. during Kick Off; SRS, LLD, Existing Study Report, Pre-Requisite Documents etc. during requirement gathering stage; UAT Plan, Test Cases, Customization Documents etc. during Implementation; User Manual, Training Manual, change request documents which includes configurations, architecture diagrams etc. and any other management support document etc. during post implementation.

xvii. The Below Mentioned requirement of the resources during the Warranty and Maintenance period is the minimum requirement, bidder is required to right size the requirement in order to meet the Scope and SLA requirement.

xviii. One – Dedicated Project Manager -100% Onsite Deployment (Head Office) during the warranty and maintenance phase, One - Solution Architect- Onsite Support to Project team on need basis, One - Security Expert- Onsite Support to Project team on need basis, Three - Support Executives -100% Onsite Deployment (General shift 9 AM to 6 PM) and One Support Executives for each remaining shifts - 100% Onsite Deployment (for the remaining hours)

xix. The Bidder should not replace resources without prior permission of UIIC. Also, the bidder should give at least one-month prior notice to UIIC in case of resource replacement. It is the duty of the bidder that the replacement provided should be equally or more qualified and experienced than the existing resource. Also, the existing resource should provide the complete handover to the new resource.

xx. During Measure & Manage period, Bidder will be responsible for:

a. Overall maintenance and working of all the Solutions and hardwares supplied
b. Bug fixing and delivery of patches/ version changes effected
c. Providing tools for creating knowledge repository for the bugs identified, resolution mechanism, version upgrade, future upgrade etc.
d. Bidder shall create the knowledge repository and shall provide UIIC Officials access to all the repository prepared for UIIC.
e. Provision should be available for version control and restoring the old versions if required by UIIC
f. Enhancement, modifications, customization, patches, upgrades due to statutory, regulatory, industry, changes will be provided at no additional cost to UIIC.
g. Configuration changes, version upgradations, performance monitoring, trouble shooting, patch installation, running of batch processes, database tuning, replacement / support, technical support for process, application and data maintenance, taking backup of the database as required, recovery, query generation and management etc. of all software supplied under this RFP document. UIIC will provide the necessary Tape Library however licenses for backup library should be in bidder's scope.
h. Immediate bug fixing should be undertaken in the event of software failure causing an interruption of operation as per the response / resolution times defined by UIIC. In case of any software /hardware failure, the solution should continue to function seamlessly.
i. All the detected errors must be notified and corrected, as per the agreed timelines

j. Support UIIC in integrating any new applications (if any directed by UIIC) with the proposed tools and provide support in extending the model and creating reports & monitoring the application/infrastructure (including software and/or hardware) from the same
k. Provide UIIC with performance monitoring reports and alert UIIC in case of any performance issues by suggesting future capacity planning
l. The operational support staff should have onsite support experience.
m. Provide BCP/DR procedures and conduct DR drills in conjunction with UIIC's policies/procedures
n. As a part of Security Measure & Manage Function the Bidder shall provide services relating to maintenance and support of hardware, software and other peripherals. Below is the list of the services required by UIIC. The list is however, not limited to these services. Also, the Bidder shall consider and envisage all services that will be required in the maintenance of these facilities and the management of these services will be provided for all offices of UIIC. The services must meet the service levels mentioned in the RFP document.
    - Coordination of warranty repair or replacement service for Hardware and process warranty claims, as applicable. If the equipment is required to be taken outside UIIC premises, the cost of transportation and other related costs will be borne by the Bidder.
    - Requesting dispatch of appropriate Vendor maintenance provider for product/Hardware maintained under a third-party agreement.
    - Coordinating and scheduling maintenance activities with the End User of UIIC (e.g. network support, facilities support, etc.)
    - Maintain accurate documentation on the current location and status of Hardware and/or software in the process of being repaired.
    - Services including requirement analysis, assisting UIIC in hardware and system software platform acquisition, testing, verification, and installation. The Bidder agrees that services provided include implementation and maintenance of the hardware as well as installation & maintenance of the software.
    - Hardware maintenance services including preventive Hardware support, preventive maintenance, corrective maintenance to remedy a problem, and scheduled maintenance required to maintain the Hardware in accordance with manufacturers' specifications and warranties.
    - Provide maintenance data, as reasonably requested by UIIC, to support replacement / refresh scheduling.
    - Provide a single-point-of-contact to End Users for the resolution of Hardware related problems or to request an equipment upgrade or consultation. If the Hardware supplied by the bidder is to be replaced permanently, then the Bidder shall replace the equipment of same Make/Model/configuration or of higher configuration at no extra cost to UIIC.
    - Provide support and assistance, as required, to isolate complex network, operational and software problems related to the proposed solutions
    - Update, or provide the information required for the UIIC to update the asset management system with the UIIC.
    - Track and report observed Mean Time Between Failures (MTBF) for Hardware.
    - Backup, remove, protect, and restore programs, data and removable storage media in a machine prior to presenting the machine for service.
    - Bidder to take corrective actions in order to resolve any security related issue including Malware attacks, Phishing attacks etc. occurring in UIIC.

o. The UIIC will not be liable to pay any additional charges in respect of any sort of maintenance required during the tenure of the contract in order to meet the scope and SLA.

3.2.3 AMC & ATS SUPPORT

i. The successful bidder should provide comprehensive AMC & ATS for proposed solution, including other software, associated modules, hardware and services required to meet the requirements in the RFP.
ii. The hardware should have three year onsite & comprehensive warranty and the AMC will commence from year 4 onwards post warranty period. The software should have one year onsite & comprehensive warranty and the ATS will commence from year 2 onwards post warranty period.
iii. Bidder shall be fully responsible for the manufacturer's warranty in respect of proper design, quality and workmanship of all required hardware, equipment, software etc. covered in the RFP. Bidder shall warrant all required hardware, equipment, spare parts etc. against any manufacturing defects during the warranty period.
iv. During the warranty, AMC & ATS period Bidder shall maintain the systems and repair / replace at the installed site, at no charge to UIIC, including defective components that are brought to the Bidder's notice.
v. If UIIC buys any other supplemental hardware which is of the same OEM and is OEM recommended from a third party vendor and installs it within this hardware under intimation to the bidder, then the warranty of hardware and software should not become void. However, the warranty will not apply to such supplemental hardware installed.
vi. If any Operating System or additional copies of Operating System are required to be installed / reinstalled / de-installed in association with this project, the same shall be done at no additional cost during the period of contract after due approval from UIIC.
vii. The bidder shall follow the below mentioned technical standards:
    a. Security Requirements
    b. Operating Procedures
    c. Recovery Procedures
    d. Perform an inventory of warranties and licenses in place as of the Start Date of the warranties.

    (Bidder needs to follow ISO standards for all the procedures.)
viii. The Bidder shall ensure that the warranty complies with the agreed Technical Standards, Security Requirements, Operating Procedures, and Recovery Procedures
ix. Bidder shall monitor warranties, ATS and AMC of the supplied hardware and software
x. As far as possible, the equipment should be repaired at site. Where the equipment is taken for repairs outside UIIC, a substitute should be provided and data, if any, should be transferred to the substitute machine besides creating back-up in one of the systems at UIIC DC and DR. Data in the machine being transferred should be deleted and hard disk should be degaussed before taking the device outside UIIC Premises.
xi. In the event of system breakdown or failures at any stage, relevant protection available shall be specified which would include the following:
    a. Diagnostic for identification
    b. Protection of data entered
    c. Recovery / restart facilities
    d. Backup facilities
xii. The ATS support for identified solution(s) should include the following:
    a. All minor and major version upgrades during the period of contract at no extra cost

b. Program updates, patches, fixes and critical security alerts as required
c. Documentation updates
d. 24x7x365 support for all the security application related malfunctions and ability to log requests online
e. The Bidder should have back to back agreement with the OEMs for ATS and AMC support.

xiii. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.
xiv. Bidder shall curtail the closure time for incidents and events, also ensure the periodic check-up reviews for the same.
xv. There will be a User Acceptance Testing by UIIC/UIIC Designated Officials for the tools deployed and Security Solutions wherever applicable.
xvi. The UIIC shall commence the User Acceptance Testing as and when products and services are made ready by the Bidder and a formal confirmation that the system is ready for UAT is submitted to UIIC. The results thereafter will be jointly analyzed by all concerned parties.
xvii. UAT will cover acceptance testing of all the product/services, integration with all the tools new and existing and integration of security solutions with all targeted devices/systems and /or applications (new and existing).
xviii. Once UAT of all the security tools as required in the RFP are individually completed, then a System Integration Testing shall be carried out by the Bidder to ensure the complete inter-operability of the security tools among themselves and integration with the existing infrastructure (targeted devices/systems) of UIIC.
xix. The Bidder is expected to make all necessary modifications to Security solution including customizations, interfaces, appliances, integration, software etc., if there are performance issues and errors identified by the UIIC. These deviations/ discrepancies/ errors observed will have to be resolved by the bidder immediately.
xx. Bidder to share with UIIC the following documents also:
- System Setting & Parameters document for the proposed solution.
- Design, Development and Technical document including the customization source code for any customization to be undertaken on the product proposed for UIIC.

xxi. Complete acceptance must adhere to the stipulated timelines.
xxii. The solution will not be accepted as complete if any facility /service as required is not available or not up to the standards projected by the bidder in their response and the requirement of this RFP.
xxiii. The UIIC will accept the solution on satisfactory completion of the above inspection.
xxiv. In case of discrepancy in facilities /services provided, the UIIC reserves the right to cancel the entire/part of the contract.
xxv. Bidder must design a high-level system integrated workflow pertaining to key security processes into the overall design of system which ensure minimum manual intervention

3.2.4 SECURITY COMPONENTS

3.2.4.1 PRIVILEGE IDENTITY MANAGEMENT

The proposed Privilege Identity Management solution should be able to address the following key areas but not restricted to:

i. Discovery of sensitive source and Data-Creation of an inventory through auto discovery of all operating systems and users, databases and database users, network/security devices and its users, relate data from TACACS/TACACS Plus/AD/Radius/ or any other LDAP, relate user data from files for applications deployed across the enterprise.

ii. In addition to Super-User password management (SUPM), solution must also be able to provide Shared Account Password Management (SAPM) including service accounts, application to application accounts password management and database administrative accounts management capabilities.
iii. Management of password vault for all types of users with single-sign-on functionality for all types of resources (OS / DB / Application / Network / Security). The vault must be highly secured and fail-safe.
iv. Creation / testing of policies/rules for enforcing access control and proper rights management on covered resources.
v. Reporting of activities through session recording / logging / Tracking.
vi. Reporting of deviations to the policies and access control.
vii. Integration with SOC application and SIEM solution
viii. Support Port wise Access Manager SSL/VPN.
ix. Support strong / Multi factor authentication. Currently, UIIC provides Forti Authenticator MFA, the bidder should integrate with the existing solution.
x. Support virtual infrastructure / environment.
xi. Support easy customization of approval workflows according to business needs (without requiring code changes).
xii. Complying with relevant regulatory demands and reporting of compliance percentage i.e. IRDA
xiii. Block and prohibit activities beyond approved privileges.
xiv. Raise alerts for wrongful attempts.
xv. Help enhance forensic capability along with supporting solutions.
xvi. Role base access to servers
xvii. Audit and Monitoring of Privileged Accounts
xviii. Command Level Controls of various devices
xix. Manage passwords hard-coded in configuration files, scripts, applications, and application server configurations.
xx. The Bidder is required to supply, implement & maintain PIM

SOLUTION IMPLEMENTATION

i. Implement the solution as per UIIC's requirement
ii. Configure policies as per UIIC's requirement.

SOLUTION INTEGRATION

i. Integrate PIM solution with SIEM to generate alerts for any violations
ii. The Bidder shall be responsible for providing the operational and maintenance training to the identified staff of the UIIC as and when required by the UIIC.
iii. The responsibility of integration of solutions with SIEM and other security solution, if required, lies with the bidder selected through this RFP. The UIIC shall provide adequate support to the bidder for the purpose of integration.

MONITORING

i. Monitor events from PIM and take appropriate action after approval from UIIC on an ongoing basis.
ii. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

3.2.4.2 DISTRIBUTED DENIAL OF SERVICE (DDoS)

The proposed DDoS solution should address the following key areas but not limited to:

i. Prevent all types of DDoS attacks (volumetric, protocol & application) such as, but not limited to, UDP Flood, ICMP Flood, SYN Flood, Smurf DDoS, Slowloris, HTTP Flood, Zero-day attacks, TCP exhaustion, etc. that impact the services hosted on Internet.
ii. The solution should be able to mitigate the effects of DDoS attacks over Internet links commissioned in our Data Centre and Disaster Recovery Center.
iii. The Solution should identify the root cause of the attack & take preventive action to avoid facing similar type of attacks again.
iv. Solution should detect the attack irrespective of the type of attacks such as volumetric, layer 2, 3, 4 or 7 using the solution provided by them
v. Proposed solution should have capability of Detection and Mitigation of DDoS attacks.
vi. Constantly monitor the behavior of the application visitors.

The Bidder is expected to perform the following activities:

SOLUTION IMPLEMENTATION

i. Implement the solution as per UIIC's requirement
ii. Configure policies as per UIIC's requirement.

SOLUTION INTEGRATION

i. Integrate DDoS solution with SIEM and other security solutions to generate alerts for any violations
ii. The Bidder shall be responsible for providing the operational and maintenance training to the identified staff of the UIIC as and when required by the UIIC.
iii. The responsibility of integration of solutions with SIEM and other security solution, if required, lies with the bidder selected through this RFP. The UIIC shall provide adequate support to the bidder for the purpose of integration.

MONITORING

i. Monitor events from DDoS and take appropriate action after approval from UIIC on an on-going basis.
ii. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

3.2.4.3 DATABASE ACTIVITY MONITORING (DAM)

The proposed Database Activity Monitoring solution should be able to address the following key areas but not restricted to:

i. Creation of an inventory through auto discovery of all databases and database users, deployed across the enterprise. Discovery of sensitive data.
ii. Creation of policies/rules for enforcing access control and proper rights management on databases.
iii. Monitoring access to databases, database activities, blocking unauthorized access/activities and segregation of duties.
iv. Reporting of deviations to the policies and access control.
v. Complying with relevant regulatory demands.
vi. Help enhance forensic capability along with supporting solutions
vii. The Bidder is required to supply, implement & maintain DAM

SOLUTION IMPLEMENTATION

The Bidder is expected to perform following activities:

i. Deploy the DAM for DC and DR locations for the in-scope databases
ii. Configure the DAM rules and policies.

SOLUTION INTEGRATION

i. Integrate DAM with SIEM to generate alerts for any DAM violations and provide a correlated view of threats and vulnerabilities associated with them along with remediation mechanism.
ii. The responsibility of integration of the DAM solution with SIEM and any other solution, if required, lies with the Bidder selected through this RFP. The UIIC shall provide adequate support to the Bidder for the purpose of integration.

MONITORING

i. Monitor events from DAM and suggest/ take appropriate action to the UIIC on an on-going basis.
ii. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.

3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)

The SIEM solution is expected to collect logs from security and network devices, servers and application security logs. In addition, the logs being generated by the solutions deployed as part of the SOC implementation need to be collected by the SIEM. The bidder is expected to perform the following as part of the SIEM:

SOLUTION IMPLEMENTATION

The Bidder is expected to perform following activities:

i. Prepare the designs and implement the solution in line with IRDAI's guidelines on Information and cyber security for Insurers, ISO27001:2013/ ISO22301/IT Act (along with its amendments) standards as modified from time to time.
ii. Deploy and Implement the SIEM for DC and DR locations for the in-scope identified devices/applications/databases etc.
iii. This will also include integration of the solution with all devices such as routers, switches, servers, firewalls, DDoS appliance, Load Balancers, WAF, and APTs etc. (This list is not exhaustive). UIIC may at its discretion add the security solution/devices which has to be integrated by the bidder during the contract.
iv. Creating and applying policies after analyzing traffic pattern for correlation purpose
v. Develop parsing rules for non-standard logs
vi. Implement correlation rules based on out-of-box functionality of the SIEM solution and also based on the standard use-cases.

SOLUTION INTEGRATION

i. Integrate SIEM with various applications and solutions
ii. The responsibility of integration SIEM lies with various applications and solutions with the Bidder selected through this RFP. The UIIC shall provide adequate support to the Bidder for the purpose of integration.
iii. Integration with TACACS/TACACS Plus/AD/Radius/ or any other LDAP to facilitate user identification.
iv. Integration with Security and Network Solution and Appliances

v. Integration with Server, Storage, VM etc. to provide the consolidated view of the events
vi. Configure all automated updates for all features by the SIEM solution.
vii. Configuration of update and upgrades as and when the latest version is released.
viii. Configuring backup Schedule of the SIEM solution.
ix. Check for Failover between appliances used for SIEM solution.

MONITORING

i. The SIEM should be able to collate logs from the devices/applications/databases/servers/all the integrations points etc., including the solutions deployed as part of this RFP
ii. Improve the policies configured on an on-going basis to reduce the occurrence of false positives.
iii. Configure Incident based alert mechanism supported by devices/application like Visual Alerts, e-mail etc.
iv. The SIEM should be able to log automated tickets on Ticketing Tool based on the criticality and threshold defined.

ONGOING OPERATIONS

i. Monitor the SIEM alerts and suggest/take appropriate action
ii. Perform on-going optimization, performance tuning, maintenance, configure additional use-cases, suggest improvements as a continuous improvement process, trend Analysis etc.
iii. Perform log backup and archival as per UIIC's policy requirements and applicable legal/statutory requirements of Govt. of India.
iv. Install/Re-install/ reconfigure any component/ system of the security equipment's supplied by the bidder, in case of crash of those components / system on problem or patch/upgrades etc. The bidder also needs to support, if any security installations done by a separate vendor.
v. Root cause analysis of any event has to be done and proper corrective action has to be taken with information to UIIC officials. Based on that, the bidder should recommend for improvement to policies, procedures, tools and other aspects.
vi. Creating Out-of-the-box reports and customized reports templates based on the needs of UIIC. The reports should be available for the following (not limited to):
    a). Indian Information Technology Act 2000 including all amendments
    b). IRDA guidelines
    c). Payment Card Industry (PCI)
    d). ISO27001
    e). ISO22301 etc.
    f) COBIT etc.
vii. Switches of the RO and Branches are managed and maintained by the other Vendors of UIIC, Bidder is required to coordinate with the UIIC Vendors to collect the logs manually and capture & ship the same in the SIEM Solution in order to provide comprehensive analysis of the logs. Frequency of the Log capturing has to be mutually discussed during the time of SRS Preparation and Signoff.

STORAGE

i. The Bidder is required to propose the solution in order to store 90 days logs (normalized Logs) online.
ii. In addition, after 90 days' duration the bidder should maintain logs on the TAPE Drives. The bidder is responsible for sizing the hardware and software adequately based on the EPS estimate given.
iii. The bidder is responsible for automated online replication of logs (online/ archival) from DC to DR for redundancy.

iv. The solution should be capable of automatically moving the logs from online to archival drives based on the ageing of the logs.
v. Key Applications to be monitored are as follows, but not limited to:

S. No	Applications
1	Email Exchange-Domino
2	Portals
3	GC CORE
4	SAP
5	Antivirus-Trend Micro
6	Active Directory-Microsoft
7	HSM
8	DLP - Trend Micro
9	Proxy – Barracuda

vi. The Bidder is required to right size the EPS (Events Per Second) Count based on the solution proposed through this RFP in order to handle the EPS count generated through the supplied Solutions/hardware. The EPS Count provided in the RFP is catering to the available solutions/devices with UIIC. In case the supplied solutions and/or appliance is unable to maintain the requirement during the contract period the bidder is required to augment the solution and/or hardware without any additional cost.

3.2.4.5 WAF

UIIC need WAF for web-based applications and internet-facing data. Automated protection and layered security protect web applications from sophisticated attacks such as SQL Injection, Cross Site Scripting attacks and data loss. With an application aware load-balancing engine to distribute traffic & route content across multiple web servers, the load balancing helps increase application performance, improves resource utilization and application stability while reducing server response times.

i. Scope is to setup and install a Web Application Firewall (WAF) and manage for operations and sustenance as per the subscription model.
ii. Web facing application servers will be routed to WAF for scanning.
iii. The WAF will be deployed as per the industry standards and best practices.
iv. WAF will be deployed in monitoring mode for 45 days and based on the application team from inputs – Deployment will be moved to inline.

v. To understand the application traffic pattern along with customer application team.
vi. Post analysis inline security profiles will be created to block the malicious traffic.
vii. Any Incidents with respect to application layer analysis would be notified to customer for further action.
viii. Weekly and Monthly reports will be sent to customer for review and remediation

Service Transition

To build and deploy IT services. Service Transition also makes sure that changes to services and Service Management processes are carried out in a coordinated way.

Key Objectives of Service Transition are:

- To ensure that a service can be managed, operated and supported
- To provide quality knowledge of Change, Release and Deployment Management
- To plan and manage the capacity and resource requirements to manage a release

Service Operation

To make sure that IT services are delivered effectively and efficiently. The Service Operation process includes fulfilling user requests, resolving service failures, fixing problems, as well as carrying out routine operational tasks

- Key objectives of the Operations Management function
- Swift application of skills to diagnose any IT Operations failures that occur
- Regular scrutiny and improvements to achieve improved service at reduced costs
- Maintenance of status quo to achieve stability of day to day processes and activities.

Service Management & Reporting

This process reports on the results achieved both operationally and strategically. It also reports on any developments related to Service Level Agreements such as hitting various targets, like availability. Its purpose is to provide information to both IT and the business in order for informed decisions to be made.

3.2.4.6 ACTIVE DIRECTORY MIGRATION

Migration Scope

1. **AD Migration**

   All the domain controllers will be updated to the latest version (Windows Server 2016) on a new hardware.

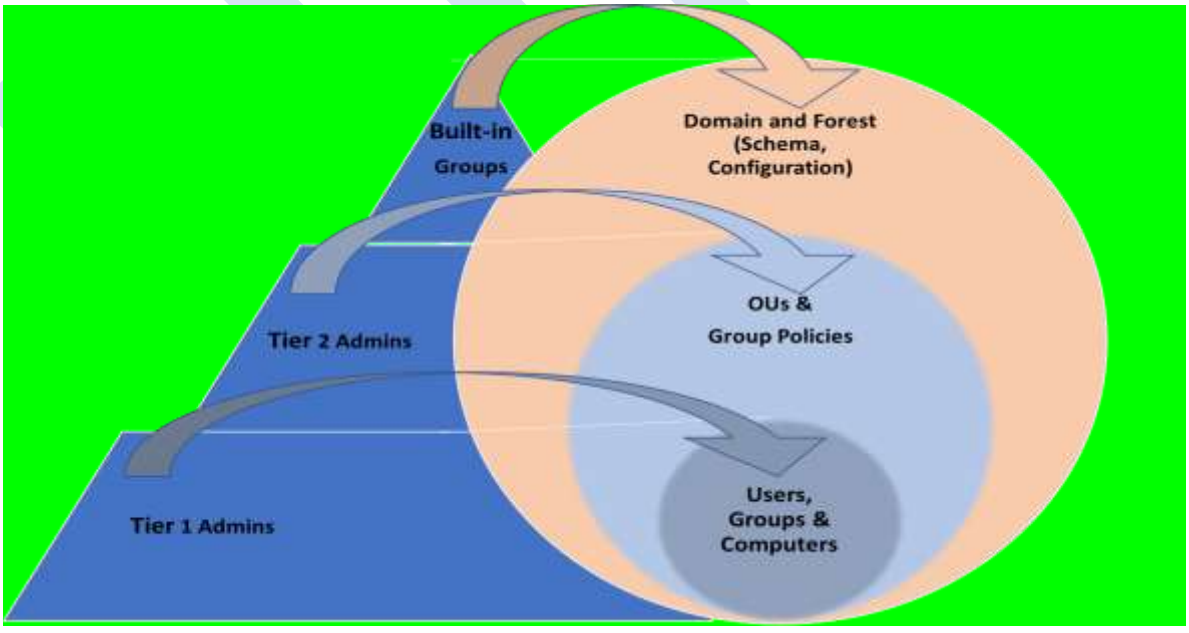
   - Active Directory Schema will be upgraded to support new features and functionalities offered by the latest version of Windows/AD

- The AD setup will be scaled up - two additional domain controllers will be installed in the primary data centers, making the overall count to 6 DCs (4 primary and 2 DR)
- All the DCs will be writable DCs (No RODCs) and hold Global Catalogue and DNS roles.
- All the Active Directory (FSMO) roles and functionalities will be transferred/distributed to the new servers, so that the old servers can be safely decommissioned with a thorough study of application and other AD integrations.
- AD integration with NTP source for Time synchronization
- Decommission of old Domain Controllers after isolating/transferring dependencies.

2. Delegation Model

AD Delegation model (Least Privileged Access) will be setup – with following categorization of permissions to manage UIIC Active Directory Setup.

- Privileged custom groups – will not have permanent members or will have manageable number of trusted administrators (One or two members from the bidder's L3 support and from UIIC) – Domain and Forest Level privileges, can manage entire domain/forest.
- Tier 2 Admins – Level two administration, who can manage OUs, Group Policies along with other AD objects within. Can be granted other AD dependent functionalities like DNS management, Sites and Services etc. – L2 Administrators from the bidder's support and members from UIIC.
- Tier 1 Admins – Level 1 Administrators with least privileges to create and modify user, group and computer objects- along with other basic AD functionalities like Password management, domain joining etc. – L1 Administrators and Service Desk.



3. AD Clean Up

AD clean-up process shall involve the following activities -

- Categorization of accounts to determine their dormant state (considering their purpose, last login information, Service category, Account Enabled State, Password State etc.)
- Disable ahead of Deletion Model - Accounts are categorized, disabled and moved to dedicated OU (Organizational Unit) ahead of deletion- followed by deletion after a specified interval.
- Standardizing the AD Cleanup process with suggested best practices for AD accounts Cleanup.
- A dedicated L2 resource with organization-wide permissions must be appointed to carry out this activity – once every 6 months

Considering the amount of time involved in studying the dependencies and categorizing the objects for their dormant state, this shall be considered outside the migration activities.

4. Application Integration with AD

The following core applications (This list is only indicative and may undergo changes as per UIIC requirements) are currently integrated with Active directory -

- Core Insurance
- SAP
- HR Systems
- VPN Authentication
- Treasury Management

Please be noted that, UIIC (Application teams) will ensure that the applications compatibility with the respective vendors for AD migration and any changes on the application side will be taken care by UIIC / Respective application owners. AD administrators / Bidder shall not be involved in any application configurations.

Bidder will provide necessary information for reconfiguring these applications from active directory perspective to ensure their integration with the upgraded version of active directory.

5. Workstation Management through AD

The workstation joining is expected to be owned by the concerned UIIC IT team, who shall be granted required credentials for joining the workstations to the domain.

- Local admin credentials provided to the users shall be disabled/deleted to avoid logins other than domain credentials. So, the users must have an active AD user account and login credential should be communicated to access the domain resources.
- Concerned IT must also ensure to copy the local profile data of the workstation users to the domain profile, for the user consumption post domain joining.

As per UIIC, a study can be conducted (outside the migration window) on other flavors (Operating System) of devices and workstations when available to understand their possibilities and limitations of managing them through Active Directory. However, this shall not be considered in the current scope of the AD migration activities as it is futuristic and UIIC currently do not have such devices in the system.

6. **Managed Services / FMS Activity for Active Directory**

   Services include end to end management of Active Directory services and related functions – which will include

   - 24x7 Monitoring and Production Support
   - Administration activities – AD and DNS
   - Regular AD health checks and auditing
   - Backup (System State) and restore activities.
   - DR drill management as applicable.
   - Capacity Management and suggestions as applicable as per customer future needs.
   - SLA & ITSM process management.

OUT OF SCOPE

The following items will be considered out of scope for the current RFP

- Issues related to Client OS or Applications
- Existing Servers (RODCs) decommission in the remote locations
- Any end user awareness/training/communications
- Any license or CALs procurement other than OS license (should be taken by the customer).
- Any item not listed in the "Scope" section above is considered as out of scope.

Solution Components

The following table illustrates the components of the solution.

Phase	Description
Assessment and Planning	• Initial Assessment • Permissions Validation • Hardware/Server Build validation
Implementation	• AD Servers Migration/Implementation • Access Controls/Delegation Setup
Decommission and KT	• Central DCs Decommission • Knowledge transfer to Operations team
AD Accounts Deletion	• Carried out once in every 6 months outside the migration timelines.

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.

4 INSTRUCTION TO BIDDERS

4.1 INSTRUCTIONS/GUIDELINES TO BIDDERS

- UIIC invites bids for "Request of Proposal (RFP) for Supply, Installation, Implementation, Integration, Maintenance and Support of Security System."
- Tender Bidding Methodology: 'Single Stage Online submission & Three Bidding System' [Eligibility Criteria Analysis, Technical Bid and 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.
- 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 enroll 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.

ONLINE SUBMISSION

a) The bidders can access the documents in the UIIC e-tendering portal https://uiic.enivida.com/HomePage/ebidSites?siteName=uiic. 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.

b) For further instructions regarding submission of bids online, the bidders shall visit the e-tender portal (https://uiic.enivida.com/HomePage/ebidSites?siteName=uiic).

c) The relevant tender documents can be purchased/downloaded from the e-tendering site with the bidders authorized user credentials.

d) The bidders should mandatorily fill in all relevant details as per the requested form in the e-tendering portal in three i.e. Eligibility Criteria Analysis, Technical Bid & Commercial Bid and all relevant scanned copies to be attached.

ONLINE DOCUMENTS TO BE SUBMITTED

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

ELIGIBILITY CRITERIA ANALYSIS DOCUMENTS (ONLINE SUBMISSION - SCANNED DOCUMENTS)

1. Tender Fee submission payment proof (Non - Refundable).
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 13 in stamp paper
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
12. Restriction of Bidders from countries sharing border with India as per ANNEXURE 11
13. Physically Sign the RFP document and attach the scanned copy.

TECHNICAL BID DOCUMENTS (ONLINE SUBMISSION - SCANNED DOCUMENTS)

1. Compliance Statement for the prescribed Technical specifications as per ANNEXURE 10. Along with all supporting documents as detailed in ANNEXURE 10.
2. Technical Documentations (if any)
3. Data Sheet of the quoted models

COMMERCIAL BID DOCUMENTS (ONLINE SUBMISSION- SCANNED DOCUMENTS)

1. Commercial Bid to be submitted as per **ANNEXURE 7**

4.2 TENDER FEE

- A non-refundable tender document fee of ₹10,000/- (Rupees Ten 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	200999095210000100ITTender
Bank Details	Indusind Bank
Remarks	TENDER_FEE_SOC<Depositor Name>

- The vendor shall provide commercial quote as per the format given in ANNEXURE 7.
- EMD of ₹50,00,000/-(Rupee Fifty lakhs 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 ₹50,00,000/- (Rupee Fifty lakhs only).
- Bank Guarantee shall be drawn in favor of "United India Insurance Company Limited" payable at Chennai.

4.3 EMD

- 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	200999095210000100ITTender
Bank Details	Indusind Bank
Remarks	EMD_FEE_SOC<Depositor Name>

- The EMD will not carry any interest.
- The electronic credit should be effected positively on the day prior to the tender submission date.
- The above account details shall be used for remitting the non-refundable tender document fee as well.

4.4 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.10,000/- only (Rupees ten thousand Only) at least two days prior to date of Pre-bid meeting.
- The interested bidders should have made the tender fee before the pre-bid meeting date to consider their queries for pre-bid meeting. No admission to pre-bid meeting for those not making tender fee payment.
- 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 has to be emailed to the following email id - 'rfp.networks@uiic.co.in'.
- Pre-bid queries should be mailed to us in the email id 'rfp.networks@uiic.co.in' in the attached format in ANNEXURE 15.
- 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 only.

4.5 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)

4.6 REFUND OF EMD

- EMD will be refunded to the successful bidder on submission of bank guarantee and agreement copy, only after completion of installation etc. in all respects to the satisfaction of the Purchaser.
- 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.

4.7 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.
- Award contracts to one or more bidders for the item/s covered by this tender.
- Seek clarifications from the prospective bidders for the purpose of finalizing the tender.

4.8 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 past experience is not satisfactory.

4.9 VALIDITY OF TENDERS

Tenders should be valid for acceptance for a period of at least 120 (one hundred and twenty) days from the last date of tender submission. Offers with lesser validity period would be rejected.

4.10 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 and 3 (THREE) months 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 website 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.

4.10.1 ACCEPTANCE OF THE SOLUTION

The User acceptance test will be carried out as per mutually agreed Acceptance Test Plan (ATP) against the systems requirements. The system will be considered accepted (supplied, installed and operationalized) only after Acceptance Test is completed.

Some of features required to be completed are enumerated below:

i. The solution should correspond to what is stated in the purchase order without deviation except where mutually agreed upon
ii. The equipment is fully installed, commissioned and operational. The features specified in the Functional Specifications / mutually agreed for implementation should be demonstrated.
iii. The final acceptance of the system will be based on successful processing under live demonstration.
iv. First acceptance will be after equipment are installed, commissioned, tested and

all features are demonstrated at the specified locations.

In case of discrepancy in hardware & related software supplied & not matching the Bill of Materials or technical proposal submitted by the bidder in their technical bid, the bidder shall be given 6 weeks' time to correct the discrepancy post which UIIC reserves the right to cancel the entire purchase contract and the Bidder should take back their equipment at their costs and risks. The test will be arranged by the Bidder at the sites in the presence of the officials of UIIC and / or its consultants and appropriate functional and technical training should be given to the officials of UIIC / or its consultants. The warranty for the equipment including all the software and other peripherals equipment & software by the Bidder pursuant to this Agreement will commence after acceptance testing. There shall not be any additional charges for carrying out this acceptance test. UIIC will take over the system on successful completion of the above acceptance test. The Installation cum Acceptance Test & Check certificates jointly signed by Bidder's representative and UIIC's official or its authorized representative should be received at Head Office along with invoice etc. for scrutiny before taking up the request for consideration of payment.

4.10.2 CONDITIONAL BIDS

Conditional bids shall not be accepted on any ground and shall be rejected straightway. If any clarification is required, the same should be obtained before submission of bids.

4.10.3 INSTALLATION AND IMPLEMENTATION

The bidder shall be responsible for supply, installation and commissioning of the proposed solution, hardware with technical specification as mentioned in ANNEXURE 10; and to undertake support of the same.

At the direction of UIIC, the acceptance test of the solution shall be conducted by the successful bidder in the presence of UIIC's authorized representative(s) and/or any other team or agency nominated by UIIC. All expenses for acceptance test shall be borne by the bidder. The acceptance tests should include verification of documentation for equipment start- up procedures; shutdown procedures; configuration; failover testing and testing of all redundancies – verification of documented fail-over and restoration procedures. Draft Acceptance test procedure should be submitted by bidder. The final acceptance test procedures will be discussed and mutually agreed after the implementation.

4.11 SECURITY DEPOSIT

The successful bidder will have to furnish a security deposit to the tune of 10% of the total contract value in the form of a Bank Guarantee for a period of 5 years & 3 months obtained from a nationalised/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. TRANSIT INSURANCE

The equipment i.e. hardware, software etc. supplied under the contract shall be fully insured in Indian Rupees by the successful bidder against loss or damage incidental to manufacture or acquisition, transportation, storage, delivery and installation. The period of insurance shall be up to the date the supplies are successfully delivered to UIIC. The successful bidder shall ensure that the insurance policy is in force and make necessary arrangement for renewal of the policy whenever required. The bidder shall not hold UIIC responsible for rejection of the insurance claims of the bidder by the insurer.

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 without any changes in unit price of the ordered 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 DC & DR Security Equipment 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 0.5% of the contract price (ANNEXURE 7, Table - Grand total) for every week (seven days) or part thereof of delay, up to maximum deduction of 10% of the contract price (ANNEXURE 7, Table - Grand total). 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 clauses 27 and 35.

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 the purpose of 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, earth quake 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.

22. WAIVER

No failure or delay on the part of any of the party relating to the exercise of any right power privilege or remedy provided under 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.

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 has to 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 has to 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.

26. PREFERENCE TO MAKE IN INDIA

Applicability of Preference to Make in India, Order 2017 (PPP-MII Order)

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.P-45021/2/2017(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.

27. 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.
The Project Manager/Coordinator shall submit weekly report on the progress of the project to UIIC and appraise the activities completed during the week and activities to be taken up in next week. Necessary

assistance from UIIC officials will be provided to ensure that activities will be completed in time. The detailed activities to be completed in each phase are mentioned below along with the timelines.

S.No.	Key Activities	Item	Time Lines
1	i. PIM ii. SIEM iii. DDoS iv. WAF v. DAM vi. AD Migration	Delivery of Hardware / appliance and licenses.	8 weeks to 10 weeks from the Date of Issuance of PO
		Installation, commissioning and Implementation	24 Weeks from the Date of Issuance of PO

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 stated below:
    a. In the event of delayed delivery i.e. delivery after the expiry of 08 weeks from the date of purchase order, the vendor shall be liable to pay a penalty, subject to a maximum of 1% (one percent) of the respective location price relating to hardware as detailed below.
        i. 0.1% for the first week;
        ii. 0.5% for the second week;
        iii. 1% for the third week and above;

    For the purpose of this clause, part of the week is considered as a full week.

d. In case the site is not ready for installation, the principle of deemed installation will apply for releasing the relevant payment on submission of SNR (site not ready) declaration.

e. 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.

f. In the event of delayed 'Power ON' i.e. expiry of 01 (one) weeks from the date of delivery of hardware at respective location, the vendor shall be liable to pay a penalty, subject to a maximum of 1% (one percent) of the respective location price relating to hardware as detailed below.
        i. 0.1% for the first week;
        ii. 0.5% for the second week;
        iii. 1% for the third week and above;

For the purpose of this clause, part of the week is considered as a full week.

g. In the event of delayed migration / commissioning / documentation i.e after 15 (fifteen) weeks from the date of power-on of hardware at respective location, the vendor shall be liable to pay a penalty at a percentage on the order value of the solution for a particular location, subject to a maximum of 5% (five percent) of the respective location price relating to hardware as detailed below.

   i. 1% for the first week;
   ii. 2.5% for the second week; and
   iii. 5% for the third week and above.

For the purpose of this clause, part of the week is considered as a full week.

28. WARRANTY & ON-SITE MAINTENANCE

i. The hardware should have three year onsite & comprehensive warranty and the AMC will commence from year 4 onwards post warranty period.
ii. The software should have one year onsite & comprehensive warranty and the ATS will commence from year 2 onwards post warranty period.
iii. Warranty for the supplied hardware will commence from the date of acceptance of the hardware by UIIC and software warranty will commence from the date of the respective solution Go-Live. Bidder is required to track of the product warranties and support from OEMs for all the supplied solution and hardware and submit the report to UIIC
iv. Performing warranty and license registration, if any, with the appropriate manufacturer, for hardware and software that are either procured through the Bidder or procured by UIIC with notification to the Bidder for inclusion in such database.
v. Reports related to hardware licenses and warranties and software licenses must be provided to UIIC
vi. All software to be supplied/ delivered and installed must be of the latest version and should form part of the OEM‟s current product line.
vii. The bidder should also ensure that the solution proposed shall be technically compliant to perform satisfactorily as per requirements mentioned in the specification and deliverables.
viii. The warranty, which for all practical purposes would mean Comprehensive On-site Warranty, shall start and remain valid for three years from the date of installation and acceptance of products.
ix. In the event of replacement of any part of the system, it should be done with a part of equivalent or higher configuration which should be compatible with the system
x. Warranty shall include software upgrades, updates, patches, hot fixes and service support without charging any additional cost to UIIC.
xi. In case of shifting of any appliance supplied by the bidder at any location of UIIC, wherever the appliance has to be shifted from one UIIC location to another, the bidder is required to uninstall / reinstall and maintain the system/s at the new location, without any extra cost to UIIC.

Bidders need to ensure that the solutions and hardware proposed comply with these minimum technical requirements. The Bidder shall provide the details of each individual solutions proposed along with the Hardware & software proposed, in ANNEXURE 7 - COMMERCIAL BID FORMAT.

Bidder should right size the hardware, software and its related services/support in order to meet the requirement as mentioned in the RFP for the entire contract. In case of shortfall bidder is required to provide the additional hardware, software and its related services/support, without any additional cost to UIIC in order to meet the requirement of the RFP.

Bidder should ensure the compliance to SLAs, Scope and Terms & Conditions as defined in the RFP for the entire contract period.

Bidder shall ensure after sales support and maintenance of the complete system to provide prescribed SLA. The bidder is to ensure that the OEM support service for the proposed software and hardware is available for the entire contract period. In case of any support/software/equipment issue, Bidder shall not only inform UIIC beforehand but also shall provide the replacement solution/equipment of same/advanced model at no cost to UIIC.
The Bidder shall be responsible for all patches/updates required in the offered solutions for smooth implementation of the project, without any extra cost to UIIC.

Sr.No.	Phase	Nature of activity	Remarks	Primary Responsibility
1	Planning	i. Conduct Kick-off meeting ii. Identify project point(s) of contact iii. Identify UIIC resources required to assist in deployment, policy walkthrough, testing, and installation. iv. Low Level Requirement Gathering v. Project Planning	Project Plan Project Governance	Bidder/OEM

2	Design	i. Bidder/OEM should execute design phase ii. Bidder/OEM should develop solution design/architect documents which will include: • Solution overview and conceptual design • Detailed design and connectivity parameters • Create a User Acceptance Test Document	Design & Architecture Document Prerequisite Document User Acceptance Test Plan	Bidder/OEM
3	Delivery	i. Physical delivery of the security equipment/ solutions as per ANNEXURE 7 – Commercial bid format at DC, DR.	The Bidder must supply and deliver the security equipment/ solutions mentioned in ANNEXURE 7 – Commercial bid format at the respective UIIC's site.	Bidder/OEM
4.	Installation & configuration	i. Deploy solution ii. Complete initial configuration iii. Complete Integration and Installations of Security Solutions with relevant applications/devices/solutions iv. Documentation of installation and configuration	The Bidder is required to provide following deliverables as part of this phase: Successful deployment Solution Installation and Configuration Document	Bidder/OEM

			Gap Assessment The Bidder/OEM is required to unpack, assemble, mount and boot the equipment and install the necessary service packs, patches, and fixes to the Operating System, set up and configure the equipment. Bidder to resolve any compatibility issues of sub-systems with OS, respective drivers, firmware, and any other cards to be installed if required.	
5.	Optimize	i. Fine-tuning of solution ii. Monitor and resolve issues iii. Provide an information knowledge- transfer workshop	Tuning policies. Policies override SOP Transfer of Information Session	Bidder/OEM
6	Deployment Confirmation and Validation	i. This phase will comprise of deployment validation to be conducted by OEM.	Validation Report by OEM	OEM

		ii. In case OEM is not satisfied with the installation and configuration of product, they will submit their recommendation in form of a report to the UIIC accordingly,		
7	Monitoring, Management & Sustenance	i. Post- deployment (after sign-off) Bidder will manage & monitor proposed solution ii. Facilitation & operation for all change management, upgrade, updates, etc. during contract period	Reports and Dashboards as per defined SLAs Go Live Operations	Bidder/OEM
8	Warranty & AMC/ATS	Provide warranty and AMC/ATS support for the tenure of the contract	The Bidder will be responsible for providing comprehensive onsite warranty support, back-to-back from the OEM to meet the Service Levels	Bidder

The Bidder shall undertake to provide an onsite & comprehensive 3 (three) Year Warranty and from year 4 onwards post warranty period for all supplied Hardware while one year onsite & comprehensive warranty and the ATS will commence from year 2 onwards post warranty for all supplied softwares at the respective locations of the Company as provided in the Purchase Order / Contract for Supply.

Preventive Maintenance: Bidder shall carry out preventive maintenance at least once in quarter in consultation with the UIIC team during the warranty period as well as in the subsequent Support period. Preventive Maintenance will include replacement of worn-out parts, checking diagnostic etc. In case equipment is taken away for repairs, the Bidder shall provide a standby equipment (of equivalent configuration or higher), so that the work of the UIIC is not affected.

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

29. PAYMENT TERMS

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 Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of UIIC.

Hardware, Software and other components to be provided for execution of project should be sized for entire contract period by considering Scope, functional & technical requirements and SLAs.
However, if it is found that the hardware is not sized adequately or the hardware utilization goes beyond the threshold limit of 80%, the Bidder must provide additional hardware at no additional cost to meet the performance parameters set by UIIC.

The scope of work is divided into different areas and the payment would be linked to delivery and acceptance. All / any payments will be made subject to compliance of Service Levels defined in the RFP document. Such withholding of payment shall not amount to a default on the part of UIIC. If any of the items / activities as mentioned in the price bid is not taken up by UIIC during the assignment, UIIC will not pay the fees quoted by the Bidder in the price bid against such activity / item.

Payment for the Supply of required Hardware, Software, Design, Installation, Implementation, and Commission of the solutions shall be made by UIIC as per the solutions in scope as mentioned in the Scope of Work.

S.No.	Activity	Payment to be released	Documents to be submitted by the bidder
1.	Hardware / Appliance	70% of total hardware cost	Delivery challan of hardware duly signed by UIIC officials
		30% of total hardware cost	On successful installation
2.	Software / License	100% on delivery of the licenses	On Delivery of Licenses
3.	Installation, Implementation & Commissioning	100% of the Installation, Implementation & Documentation	On Documentation

4.	FM Support (if applicable)	Payment will be made quarterly in arrears.	Bidder to submit the relevant documents with the attendance sheet along with the invoice
5.	ATS	100%	Payment will be made Yearly In advance
	AMC	100%	Payment will be made Yearly In advance
6.	Training	100% cost would be payable post successful completion of the training to the designated officials	On Successful Documentation

30.1 MODE OF PAYMENT

UIIC shall make all payments only through Electronic Payment mechanism (viz. ECS).

30.2 PENALTIES AND DELAYS IN BIDDER'S PERFORMANCE

In case the vendor fails to meet the SLA mentioned in section 35, penalty will be imposed as mentioned in section 35 Service Level Agreement.

30.3 DELAY IN BIDDER'S PERFORMANCE

Supply, Installation, Implementation, Integration, Maintenance and Support of Security System 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.

31. 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 that 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.

32. 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.

33. CLARIFICATION TO BIDDERS

All queries / requests for clarification from bidders must reach us by e-mail to (rfp.networks@uiic.co.in) before due date mentioned in *Section 1 - Bid Schedule and Address as* per ANNEXURE 15 – 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

- 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). It would be responsibility of the bidder to check the website before final submission of bids.

34. APPLICATION SOFTWARE

The vendor should coordinate with the application software vendor for providing access permissions in the Security Equipments to the applications installed in our network and ensure that the applications are accessible over the network.

35. SERVICE LEVEL AGREEMENT

35.1 SERVICE LEVEL

The SLA specifies the expected levels of service to be provided by the Bidder to UIIC. This expected level is also called the baseline. Any degradation in the performance of the solution and services is subject to levying penalties.
Payments to the Bidder are linked to the compliance with the SLA metrics. During the contract period, it is envisaged that there could be changes to the SLAs, in terms of addition, alteration or deletion of certain parameters, based on mutual consent of both the parties i.e. UIIC and Bidder.
The Bidder shall monitor and maintain the stated service levels to provide quality service. Bidder to use automated tools to provide the SLA Reports. Bidder to provide access to UIIC or its designated personnel to the tools used for SLA monitoring.

35.2 DEFINITIONS

1. "Availability" means the time for which the services and facilities are available for conducting operations on the UIIC system including application and associated infrastructure.
   Availability is defined as (%) = (Operation Hours –Downtime) * 100%
   (Operation Hours)
2. The business hours are 24X7 on any calendar day the UIIC is operational.
3. All the infrastructure of Data Center, Disaster Recovery site, Offices/Branches will be supported on 24x7 basis.
4. The "Operation Hours" for a given time frame are calculated after deducting the planned downtime from "Operation Hours". The Operation Hours will be taken on 24x7 basis, for the purpose of meeting the Service Level requirements i.e. availability and performance measurements both.
5. "Downtime" is the actual duration for which the system was not able to service UIIC or the Clients of UIIC, due to System or Infrastructure failure as defined by UIIC and agreed by the Bidder.
6. "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity as defined in this SLA. The scheduled maintenance time would not be during business hours. Further, scheduled maintenance time is planned downtime with the prior permission of UIIC
7. "Incident" refers to any event / abnormalities in the functioning of any of IT Equipment / Services that may lead to disruption in normal operations of the Data Centre, System or Application services.
8. Total Maintenance Cost refers to Sum of FM Manpower Cost and AMC, ATS & other Cost for the entire contract duration.

35.3 INTERPRETATION & GENERAL INSTRUCTIONS

1. Typical Resolution time will be applicable if systems/components are not available to the UIIC's users.
2. The SLA parameters shall be monitored on a monthly basis for the entire contract duration (including the warranty period) as per the individual SLA parameter requirements. The Bidder

is expected to provide the following service levels. In case the service levels defined in the tables below cannot be achieved, it shall result in a breach of contract and invoking of the penalty clause.

3. A Service Level violation will occur if the Bidder fails to meet Minimum Service Levels on a monthly basis for a Service Level.
4. Quarterly SLAs would be analyzed. However, there would be month wise SLAs and all SLA targets must be met on a monthly basis.
5. Overall Availability and Performance Measurements will be on a quarterly basis for the purpose of Service Level reporting. Month wise "Availability and Performance Report" will be provided by the Bidder for every quarter in the UIIC suggested format and a review shall be conducted based on this report. Availability and Performance Report provided to UIIC shall contain the summary of all incidents reported and associated performance measurement for that period.
6. The primary intent of Penalties is to ensure that the system performs in accordance with the defined service levels. Penalties are not meant to be punitive or, conversely, a vehicle for cutting fees.

35.4 SERVICE LEVEL CRITERIA

Severity Definition during Live operations due to Infrastructure/Functional issues of the proposed solution, the SLA will be applicable post go-live of Solution at DC, DR and other UIIC Offices

During the term of the contract, the bidder will maintain the equipment/components/ hardware/software in perfect working order and condition and for this purpose bidder will provide the repairs and maintenance services as required.

Level Classification

Level	Function / Technologies
Critical	i. Such class of errors will include problems, which prevent users from making operational use of solution. ii. Security Incidents iii. No work-around or manual process available iv. Financial impact on UIIC v. Infrastructure related to providing solution to the UIIC users comprising of but not limited to the following: • Proposed Solution Tools / Application Servers • Proposed Solution Database Servers / Appliance • Proposed Solution servers/appliances • Network components, if any proposed by the bidder
High Priority	i. Any incident which is not classified as "Critical" for which an acceptable workaround has been provided by the Bidder or; ii. Any problem due to which the infrastructure of the proposed solution is not available to the UIIC users or does not perform

	according to the defined performance and query processing parameters required as per the RFP or; iii. Users face severe functional restrictions in the application irrespective of the cause. iv. Key business infrastructure, systems and support services comprising of but not limited to the following: • Proposed solution Test & Development and Training Infrastructure and Application • Infrastructure for providing access of dashboards etc.
Medium Priority	i. Any incident which is not classified as "High Priority" for which an acceptable workaround has been provided by the Bidder; ii. Moderate functional restrictions in the application irrespective of the cause. Has a convenient and readily available workaround. iii. No impact on processing of normal business activities iv. Equipment/system/Application issues and has no impact on the normal operations/day-to-day working. v. All other residuary proposed solution Infrastructure not defined in "Critical" and "High Priority"
Low Priority	All other residuary proposed solution Infrastructure not defined in "Medium Priority "," Critical " and "High Priority"

Sr. No.	Service Area	Service Level	Penalty
1.	All Solutions Uptime	Uptime % calculated on monthly basis for each solution. In case of any hardware problems, the SI should ensure that replacement devices are made available to meet the SLAs.	Penalty (as mentioned below) of the individual quarterly maintenance Cost (Including AMC and ATS Cost). These penalties will be deducted against any payable amount by UIIC. Quarterly Maintenance Cost = (Total Maintenance Cost (Including AMC & ATS Cost) for the entire contract period) / (Contract Period *4)
		99.9% and above	NA
		98% to 99.89%	1%
		95% to 97.99%	5%
		90% to 94.99%	8%
		Less than 90%	10%
2.	Incident Response	24x7 monitoring of all in-scope devices Categorization of events into Critical, High, Medium and	All Critical, High and Medium priority incident should be logged as incident tickets and responded as per below SLAs: Incident along with action plan/

		Low priority shall be carried out in consultation with the UIIC during the contracting phase. Example for calculation of percentage of incidents 10 Incidents are logged of which 8 are responded within the specified time and 2 have been delayed. This means 8/10*100 = 80% have been Responded within the Specified timelines and correspondingly the penalty will be applied based on the event/incident categorization	mitigation steps should be provided to designated UIIC personnel as per the below SLA: • Critical incidents within 15 minutes of the incident identification. Update should be provided every 30 minutes till the closure of the incident. • High priority incidents within 30 minutes of the incident's identification. Update should be provided every 1 hour till the closure of the incident • Medium priority incidents within 60 minutes of the incident's identification. Update should be provided every 4 hours till the closure of the incident. Quarterly Maintenance Cost = (Total Maintenance Cost (Including AMC & ATS Cost) for the entire contract period) / (Contract Period *4) **Penalty:** SLA is measured on a Quarterly basis and the penalty is as follows; if Not Compliant with mentioned percentage. **Critical Events:** • 95-99%: 5% of the Quarterly Maintenance (Including ATS & AMC) Cost • 90-95%: 8% of the Quarterly Maintenance (Including ATS & AMC) Cost • <90%: 10% of the Quarterly Maintenance (Including ATS & AMC) Cost

			High Priority Events: • 95-99%: 2% of the Quarterly Maintenance (Including ATS & AMC) Cost • 90-95%: 5% of the Quarterly Maintenance (Including ATS & AMC) Cost • <90%: 8% of the Quarterly Maintenance (Including ATS & AMC) Cost **Medium Priority Events:** • 95-99%: 1% of the Quarterly Maintenance (Including ATS & AMC) Cost • 90-95%: 2% of the Quarterly Maintenance (Including ATS & AMC) Cost • <90%: 5% of the Quarterly Maintenance (Including ATS & AMC) Cost
3.	Incident Resolution	Response and resolution of the identified incidents. Managing the devices and fine-tuning them so as to avoid and prevent further attacks.	The timelines required for resolution of Critical, High and Medium priority mentioned below: • Disaster or Critical incidents within 60 minutes of the incident identification - Update should be provided every 30 minutes till the closure of the incident • High priority incidents within 90 minutes of the event identification - Update should be provided every 1 hour till the closure of the incident. • Medium priority incidents within 120 minutes of the event identification - Update should be provided every 4 hours till the closure of the incident.

			Quarterly Maintenance Cost = (Total Maintenance Cost (Including AMC & ATS Cost) for the entire contract period) / (Contract Period *4) **Penalty:** • Any violation in meeting the SLA requirements which leads to Critical incident, UIIC shall impose a penalty 10% of the Quarterly Maintenance Cost for each 30 minutes delay up to 2 hours, beyond 2 hours penalty would be 10% of the overall Quarterly Maintenance Cost for each 20 minutes delay. • Any violation in meeting the SLA requirements which leads to High or Medium incident, UIIC shall impose a penalty of 5% of the Quarterly Maintenance Cost for each 45 minutes delay up to 3 hours, beyond 3 hours penalty would be 10% of the overall Quarterly Maintenance Cost for each 30 minutes delay.
4.	Report and Dashboard	Periodic reports to be provided to UIIC	**Daily Reports:** Critical reports should be submitted as and when required. Timings will be mutually decided. **Penalty:** Delay in reporting for daily report for more than 6 hours shall incur a penalty of INR 500 for each default. **Weekly Reports:** Every Monday of the subsequent week **Penalty:** Delay in reporting by more than 3 days for weekly reports shall incur a

			penalty of INR 1,000 for each default. **Monthly Reports**: 5th of each month. **Penalty:** Delay in reporting by more than 7 days for monthly reports shall incur a penalty of INR 1,500 for each default
5.	Continual Improvement	• The Bidder is expected to improve the operations on an on-going basis. • The Bidder is expected to provide a quarterly report of the new improvements suggested, action plans, and the status of these Improvements to the UIIC. • Improvement areas could include process changes/ training resulting in efficiency/SLA improvement, new correlation rules to identify threat patterns etc.	Quarterly reports need to be provided by the 5th day of each quarter beginning Quarterly Maintenance Cost = (Total Maintenance Cost (Including AMC & ATS Cost) for the entire contract period) / (Contract Period *4) **Penalty:** Delay in providing quarterly reports shall lead to 2% of Quarterly Maintenance Cost
6.	Periodic Review	The Project Manager from the Bidder is expected to conduct a monthly review meeting with UIIC officials resulting in a report covering details about current SLAs, status of operations, key threats and new threats identified, issues and challenges etc.	• Monthly meeting for the entire contract period to be conducted on the 5th (tentatively) of each month during the operations phase. Quarterly Maintenance Cost = (Total Maintenance Cost (Including AMC & ATS Cost) for the entire contract period) /(Contract Period *4) **Penalty:** • A delay of more than three days will incur a penalty of 1% of

			Quarterly Maintenance Cost.
7	Security Device Management and Administration	Bidder is expected to provide this service on 24/7 basis. Management and administration of all in-scope security devices and/or solutions	**Penalty:** • For more than 1-hour delay (after UIIC confirmation) for rule modification in any of the security devices / solutions will incur a penalty of INR 10,000 for each default. • For wrong rule modification in any of the security solutions will incur a penalty of INR 10,000 for each default. • For a wrong rule modification in any of the security solutions by which UIIC incur any service disturbance will incur a penalty of INR 20,000 for each default.

Resources Deployment SLA

Service Details	SLA Measurement	SLA	Penalty	Measurement Tools	Remarks
Program Manager	No change in these resources for minimum 1 year from the issuance of the PO and maximum 2 changes in the complete contract term (*the Program Manager should not be rotated to other clients of the Service Provider under the contract period).	100%	Penalty shall be INR 2, 00,000 for each default beyond the agreed threshold.	Manual	If the resource leaves because of attrition, the same would not be considered for any penalty computation.
Staff transition period (Handover period)	As per below mentioning staff transition period: • Program Manager - 60 Days • Other Staff- 30 Days	100%	Program Manager/Delivery Manager- Penalty shall be INR 10,000 for each week of default or part thereof Other Staff- Penalty shall be INR 2,000 for each week of default or part thereof	Manual	
Resource Availability	Attendance for support personnel. (covers all the locations) Minimum attendance level during any shift is 100% of agreed deployment.	No. of shift Below minimum - attendance level	Penalty shall be INR 5,000 for every 2% default or part thereof below the agreed threshold	Manual	

35.5 PENALTY

i. UIIC will impose a penalty, of Rs. **20,000/- (Rupees Twenty thousand only) per week** or part thereof, for delay in not adhering to the time schedules for closing the intimated gaps for the proposed solutions identified through VAPT Report.

ii. The UIIC expects the Bidder to complete the scope of the project as mentioned in section 03 - scope of work of this document within the timeframe specified in Section 27 Project Timelines of this document. Inability of the Bidder either to provide the requirements as per the scope or to

meet the timelines as specified would be treated as breach of contract and would invoke the penalty /LD clause.

iii. Inability of the Bidder to provide services at the service levels defined would result in breach of contract and would invoke the penalty clause

iv. Notwithstanding anything contained above, no such penalty will be chargeable on the Bidder for the inability occasioned, if such inability is due to reasons entirely attributable to the UIIC.

v. Bidder needs to deploy the same resources or resources with equivalent/higher skill sets as per the terms and conditions of the RFP. For Each Default, UIIC may levy the penalty of **Rs**. **1,00,000** quarterly till the Bidder deploys the required resources

vi. The Bidder is required to provide and implement the regular updates/upgrades/patches released by the OEM within the timelines as mentioned, UIIC will levy the penalty of Rs. 20,000 per week or part thereof in not adhering the schedules.

vii. If during the contract period, any equipment has a hardware failure on four or more occasions in a quarter, it shall be replaced by equivalent or higher new equipment by the bidder at no additional cost to UIIC.

viii. The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the UIIC such as termination of contract, invoking performance guarantee and recovery of amount paid etc.

ix. The UIIC reserves the right to recover the penalty from any payment to be made under this contract.

x. The penalty would be deducted from the quarterly payouts and the cap on any penalty due during the Warranty period will be adjusted against the payments made for bills/invoices provided by the bidder. Quarterly penalty will be 20% of the quarterly payout. **For the purpose of this RFP, the total of penalties as per SLA and the Liquidated damages will be subject to a maximum of 10% of the overall contract value.**

xi. Performance measurements would be assessed through audits or reports, as appropriate to be provided by the Bidder e.g. utilization reports, response time measurements reports, ticket details and resolution time report etc. The tools to perform the audit will need to be provided by the Bidder. Audits will normally be done on regular basis or as required by UIIC and will be performed by UIIC or UIIC appointed third party.

35.6 EXCEPTION

UIIC shall not hold the Successful Bidder responsible for a failure to meet any Service Level if it is directly attributable to:

i Execution of the disaster recovery plan/business continuity plan for an UIIC declared disaster situation; and

ii Any established inability of other third-party vendor or service provider of UIIC, to fulfill the requirements as per the contract.

ANNEXURE 1 - FORMAT FOR LETTER OF AUTHORIZATION

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

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

Ref. No: 000100/HO IT/RFP/138/2020-21

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 "SUPPLY, INSTALLATION, IMPLEMENTATION, INTEGRATION, MAINTENANCE AND SUPPORT OF SECURITY SYSTEM" 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/138/2020-21

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/138/2020-21 "REQUEST FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, IMPLEMENTATION, INTEGRATION, MAINTENANCE AND SUPPORT OF SECURITY SYSTEM"

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, IMPLEMENTATION, INTEGRATION, MAINTENANCE AND SUPPORT OF SECURITY SYSTEM".

(Authorized Signatory of Bidder)

Date:

(Company Seal)

ANNEXURE 3 - MANUFACTURERS AUTHORISATION FORMAT

(To be submitted on OEMs Letter Head)

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

Ref. No: 000100/HO IT/RFP/138/2020-21

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 Supply, Installation, Implementation, Integration, Maintenance and Support of Security System"

<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.

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/138/2020-21

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/138/2020-21 - "Tender for Proposal (RFP) for Supply, Installation, Implementation, Integration, Maintenance and Support of Security System"

Dear Sir,

There are no deviations (nil deviations) from the terms and conditions of the tender. All the terms and conditions of the tender are acceptable to us.

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 "Supply, Installation, Implementation, Integration, Maintenance and Support of Security System"(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 ₹ 50,00,000/- (Rupees Fifty 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₹ 50,00,000/-
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 FORM

[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/138/2020-21

ELIGIBILITY CRITERIA FOR BIDDERS

S.No.	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
2017-2018		
2018-2019		
2019-2020		

S.No.	Eligibility Criteria	Documentary Proof Required	Bidder/ OEM	Compliance (Y/N)
a.	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 31.03.2020.	Copy of the Certificate of Incorporation issued by Registrar of Companies.	Bidder	
b.	The Bidder should be ISO 9000/9001, ISO 20000 and ISO/IEC 27001 certification holder company, with certifications valid at the time of bid submission.	Photocopies of the certificates to be provided.	Bidder	
c.	The bidder should have an average annual financial turnover of at least ₹ 200 Crore for the last three financial years viz. 2017-18,	Audited financial statements / Certificate from	Bidder	

	2018-19 and 2019-20.	Auditor		
d.	The bidder should have made Net Profit (Profit After Tax – PAT) after taxation in any of the last three financial years viz. 2017-18, 2018-19 and 2019-20.	Audited financial statements / Certificate from Auditor	Bidder	
e.	The bidder should not have been blacklisted/debarred by any Government Department, Agencies or Public Sector Undertakings in India as on the date of submission of the tender	As per ANNEXURE 2	Bidder	
f.	The Bidder should have implemented or have under implementation, minimum 3 of the below mentioned security solutions for atleast 1 BFSI Customer in india with minimum 1000 offices/Branches i.PIM ii.SIEM iii.DDoS iv.WAF v.DAM	Successful completion certificates or Credential Letters Or Copy of Contract / Purchase order from the Client for implemented projects Or Copy of Contract / Purchase order for under implementation projects	Bidder	
g.	Bidder should be providing SIEM Solution to minimum 2 BFSI customers in India	Purchase order copy / Project Sign off document /Client Certificate should be attached as proof.	Bidder	
h.	The bidder must have minimum five (5) IT Security professionals on their payroll with certification in CISA / CISSP / CISM / CEH / CCSA.	Self-Declaration/ Undertaking to this effect to be submitted by the bidder	Bidder	
i.	The Bidder must warrant that key project personnel to be deployed in this project should have managed a similar project (SIEM/DAM/DDoS/PIM/WAF) in the past.	Self-Declaration/ Undertaking to this effect to be submitted by the bidder and Details of the personnel indicating their qualifications, professional experience and projects handled.	Bidder	
j.	Bidder should be either Original Equipment	Authorization letter on	Bidder/	

	Manufacturer (OEM) of Security devices/software solutions or authorized partner of OEM. In case the bidder is an Authorized partner of the OEM, Bidder must submit the authorization letter from each of the OEM for the solutions proposed.	OEM's letterhead as per ANNEXURE 3.	OEM	
k.	Each of the proposed OEM solution mentioned below should have been implemented and running in at least 2 BFSI customers with more than 1000 branches each in India not necessarily by the same bidder. • SIEM • PIM • DAM • WAF • DDoS	Purchase order copy / Project Sign off document / Client Certificate should be attached as proof.	OEM	

Signature :

Name :

Designation :

ANNEXURE 7 - COMMERCIAL BID FORMAT [ALL AMOUNTS SHOULD BE IN INR]
[To be included in Cover 'C'- Commercial Bid]

A. Product : Hardware / Software / License / Services							AMC / ATS					TOTAL
S. No.	*Description	OEM/ SI	HW / SW / Lic / Service	Qty	Unit Rate	Total	Year-1	Year-2	Year-3	Year-4	Year-5	
1	PIM											
3	SIEM											
2	DDoS											
4	WAF											
5	DAM											
6	AD – Cleanup Activity		Service	2								
7	Any other item, if any											
8	Any other item, if any											
9	Any other item, if any											
TOTAL (A)												

***Note:** The L1 bidder should submit the bills separately for above mentioned categories. UIIC has the right to ask the detailed breakup (Hardware, Software, OS, License, Services etc.) for any of the above mentioned product/services.

B. Active Directory												TOTAL
S. No.	Description	OEM	HW/SW/Lic	Qty	Unit Rate	Total	Year-1	Year-2	Year-3	Year-4	Year-5	
1	Server		HW									
2	Windows 2016		LIC									
3	Any other item, if any											
TOTAL (B)												

C. Resources									TOTAL
S. No.	Description	Qty	Unit Rate	Year-1	Year-2	Year-3	Year-4	Year-5	
1	Project Manager at UIIC HO (Mon-Fri, 9:00 - 18:00 hrs)	1							
2	Support Executive (L1) for HO (Mon-Fri, 9:00 - 18:00 hrs)	1							
3	Support Executive (L1) for DC Primary	3							
4	Support Executive (L1) at HO / DC for Active Directory (Mon-Fri, 9:00 - 18:00 hrs)	-							
TOTAL (C)									

D. SOC Implementation		
S. No.	Description	Total
1	PIM	
2	SIEM	
3	DDoS	
4	WAF	
5	DAM	
6	Active Directory Migration	
7	Training	
TOTAL (D)		

GRAND TOTAL (A+B+C+D)	

All prices quoted are exclusive of Taxes and in INR Only.

ANNEXURE 8 - NDA (NON - DISCLOSURE AGREEMENT FORMAT)

(To be submitted in separate ₹100 stamp paper)

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

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 section 8 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 into 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 --- In the presence of: Witnesses - 1: Witnesses - 2:	(a) for & on behalf of (BIDDER'S NAME) --- In the presence of: Witnesses - 1: Witnesses - 2:

ANNEXURE 9 - VOLUMETRIC

Sr. No	Solution	Sizing Requirement
1	Privilege Identity Management	• HA at DC & HA at DR • No of resources to be connected through the PIM solution: (the above includes OS/NW/DB/Application/others in DC/DR sites) – 1800 Devices scalable to 2200 Devices, Storage 1 at DC & 1 at DR, Applications -8 Scalable to 15 and Production Database Instances – 8 scalable to 20 • No of privileged Users 100 Users Scalable to 200 User
2	Distributed Denial of Service	• HA at DC & HA at DR • Inspection throughput of 1 Gbps scalable to 3 Gbps
3	Database Activity Monitoring	• HA at DC & HA at DR • No of Active Database cores – 140 Scalable to 350 • No of Active Database instances – 7 Scalable to 20 • No. of User – 25 with scalability to 40
4	Security Information and Event Management	• HA at DC & HA at DR • EPS - 10000 Scalable to 20000
5	Web Application Firewall	• HA at DC & HA at DR • should support 5 Gbps L7 throughput and should be scalable to 10 Gbps L7 throughput or higher with additional license • should support minimum 600K Layer 4 Connection Per second • Should support minimum 800K Layer 7 Request Per second • should support minimum of 15000 SSL CPS with 2K bit key upgradable to 18000 SSL CPS • solution should support at least 8000 ECC CPS on same device

ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS

A. PIM

A. PIM			
Sr. No	**Functional Requirements (minimum)**	**Compliance**	**Remarks (Yes/No)**
	Architecture		
1	Should be Agent based/ agentless		
2	Solution should support High Availability/Redundancy deployments for higher availability and DRBC solution. The system should be highly available (24x7x365) and redundant from hardware failure, application failure, data failure, and / or catastrophic failure. The system should have provisions to keep the solution running at 100% with proper alerting, fail-over, bypass in equally secure manner with availability of credentials.		
3	The password vault must be highly reliable, the switch over to HA/DR should be instantaneous without manual intervention, and provisions should be available to recover credentials securely in case of catastrophic failures.		
4	Solution also support for printing of password in secure manner		
5	The solution should provide a secured process for encrypted storing and backups.		
6	The architecture should support network load balancing and clustering technology.		
7	If a back-end database is used/required, the database should be managed within the solution and no outside DBA access should be available. The solution needs to be fully self-managed and hardened.		
8	The platform should be highly secured/encrypted tamper-proof for the solution and for the storage. The solution should provide web-based interface for easy access and management.		
	Performance and scalability		
9	The solution should be able to be implemented in virtual environment. Solution should also be able to control, manage privileged accounts and identities on Hypervisors/ platform virtualization software (Installation on virtual servers and control of users and resources in virtual servers etc.).		
10	The product should be capable of handling 100 user accounts and 100 systems. There should be no latency or performance degradation in using an average of 100 users.		
11	In multi-tiered architecture the solution should have the capability to deploy the password database, management console, web server and reporting database etc. on separate machines which can be connected to a central management console. (Web-based Central administration within unified suite, single user interface, central		

	repository)		
12	The solution should provide scalability through a modular design for adding capacity and scalability metrics. It should have capability to integrate with HR applications / Identity and Access Management applications or Physical access applications that UIIC may procure.		
Discovery of Systems, Accounts and Services			
13	The product should be capable to dynamically and automatically detect new resources / locations like desktops, servers, operating systems, services, IIS service accounts, network devices, hyper visors in virtual systems etc., throughout the environment and provision them to the product and automatically discover privileged accounts and enforce the right password policy.		
14	Product must support open API / provide API's to add "connectors" to manage devices that are not currently supported 'out-of-the-box'. It should also be capable of connecting to legacy applications.		
15	The solution must be able to support/manage privileged accounts and create seamless single sign on in the following: Windows, Unix, HP UX, Different flavours of Linux, Oracle, MS SQL Server, SOC application like ASA-Firewall, Radware Alteon -WAF & Load Balancer, WSA -Proxy Server, Network Devices (routers, switches, firewall, IDS/IPS etc.)- Cisco, Brocade, ASA, Applications - SAP, PeopleSoft, Virtual Servers like Oracle Virtualisation ,HyperV, VMWare, web- based or client-server application, Apache, MS Exchange client support application like TOAD, SQL Plus, SSH and ODBC services/devices, Servers, PCs and Laptops connected to the network, Mobile/smart devices/applications, Middleware like Oracle WebLogic, IBM WebSphere, JBoss, Tomcat SSL/VPN application like Portwise Access Manager SAN storage devices and Tape libraries etc. or any other solution procured by UIIC during contracted period. The solution should be capable of providing multi-domain access.		
16	Should be able to seamlessly connect to Active Directory and LDAP-Compliant directory services accounts, TACACS/TACACS+ and RADIUS. For identity consolidation, solution should provide AD bridging capabilities over heterogeneous non-windows platforms as this helps to manage Unix, Linux and other non-windows platform accounts through Microsoft AD thereby enabling consolidation of authentication and account information.		
17	The solution should be able to bulk-import system lists and make ad-hoc entries through the management console.		
18	The product must be able to manage remote target systems through a firewall (e.g. servers in a DMZ, remote locations etc.) through secure built-in connectivity (without requirement of additional security; such as third party VPN)		
Password Management / Credential management			
19	The solution should have a strong inbuilt password vault/management system with single-sign-on feature. Password		

	vault should be replicated over a secured channel and off-site data backup, data restoration capabilities should be offered. PIM solution as a whole and specially the password vault, should be installed on a highly secure/ hardened system with minimal services running, in a physically safe environment with least number of people having access to the administrative controls.		
20	Should be able to create flexible password management policies for assets. A policy can be applied to an object/a group of objects or a group of policies can be applied to an asset/group of assets/objects.		
21	After dynamically discovering resources /services/ processes, the solution should be able to propagate password changes to relevant targets across the network to avoid the potential service disruptions and lockouts whenever changes are made.		
22	Product should allow bulk operations to be performed on managed accounts (such as force password change immediately, reconcile password, verify password)		
23	Password changes can be scheduled. Solution must protect password change process against race conditions like a failed attempt to update password on target system (password in vault should not be updated) or inability/ delay in determining if the password has successfully been updated on target systems or application configuration files (old password shouldn't be removed from the vault). Recovery of managed systems from a backup media should also be supported by solution - for e.g., a database recovery to a point 5 days back.		
24	Any failed password change event or exceptions should be promptly reported after a certain numbers of retries.		
25	The solution should have the capability to reset individual passwords or groups of passwords on-demand, and to schedule automated checks to ensure that each password stored in the database correctly matches the current login for each target account.		
26	The solution should keep the passwords in very strong encrypted form. Support for Hardware Security Modules (HSMs) should be available. The solution should also provide for strong encryption inside the system components/processes, between its distributed modules, and between the web application and user machines, to protect passwords and other sensitive information.		
27	Solution should be able to change password on demand, based on a specific criteria or policy, automatically or manually, support password verification, reconciliation and reporting, set password parameters like constitution, history, and change timings.		
28	The solution should support transparent connection to the target device, without seeing the password or typing it in as part of the connection.		
29	The solution should be able to manage credentials in well- known operating systems, applications, Database Management Systems, programming languages/scripts (Eg: C++, Java, .Net, VB etc.).		
30	The solution should be able to manage passwords stored in plain or encrypted, hardcoded in system files or user- defined files, database tables, network devices etc. including within application configuration files, code or scripts.		

31	The solution should have provisions to provide credentials for authenticating applications/scripts during run-time.		
Access Management			
32	The solution should be able to automatically and dynamically provision users in real time with trusted Windows domains, popular directories such as AD/ LDAP /TACACS+/RADIUS servers in accordance to the user entitlements and access privileges granted (based on least privileges principle). Solution should be able to support granular command filtering or context-sensitive entitlements on various platforms for super-user privileged management. Solution should also be able to detect and support concurrent login to managed systems as a privileged user		
33	The solution should be capable of organizing / grouping target server / device accounts into logical groups and apply granular/fine-grained access control to access the individual accounts or the groups of accounts.		
34	The solution must support full Segregation of Duties - e.g. roles are clearly and unambiguously defined with no overlapping. In addition to user access roles and entitlements, solution should also support role based administrative access in order to provide Segregation of Duties for administrative management and control. The user permission should be only as per his original privilege even he 'SU'es after logging in to the OS. Using root user credentials does not provide root privileges. Capability to restrict users to use RDP to other endpoints.		
35	It should be capable of having dual control systems (maker-checker) for approval and authorisation of critical operations with 4-eye principles.		
36	The solution should have login security by limiting user login by parameters like originating IP address, terminal ID, type of login program or time of the day or geographical location etc. and limit concurrent login sessions by user.		
37	The solution should be capable to have command level restrictions, i.e. of assigning specific commands to be run by specific users/groups, from specific nodes etc. The solution should be able to block commands from command line and in queries as configured for users/groups/target resources.		
Workflows			
38	The solution should be capable of integrating with a Change Management /ticketing system like Sapphire in order to initiate access approval workflows for scheduled changes and be able to control required access (based on least privilege principle) and monitor and/or terminate super user connections that exceed pre-set time limits (change window).		
39	It should have ability to enforce approval workflow only to the human users which can be created to a very granular level.		
40	It should support a workflow approval process that is flexible to assign multiple approvers based on product or model (I.e. require 2		

	or more approvals before access is allowed). Solution should also be able to provide delegation of management tasks like approval / review etc. Should support easy customization of approval workflows according to business needs (without requiring code changes). Solution should also be able to support emergency/ break glass scenarios.		
Auditing/Reporting			
41	The solution should provide a central live Dashboard covering features like management of devices, events and password policies, user activities, event logs etc.		
42	The system should have all regular pre-configured report templates like entitlements reports, user activities, privileged accounts inventory, applications inventory, compliance reports etc., capability to create custom reports based on users, events, activities, target systems, password uses and status etc., distribute the reports to intended users through e-mail, the ability to run all reports by frequency, on-demand and schedule them.		
43	The reports generation should support CSV or Excel. This report extraction should not have any performance impact & feature for report extraction should be available on demand & scheduled. The solution should support customizable reports.		
44	The solution should record access to the Web console for password requests, approvals and check-out, delegation changes, reporting and other activities, access to its management console for configuration and reporting, and all password change job activity.		
45	The solution should be able to record sessions, take video recording of screen shots, key strokes / commands and output, replay sessions for forensic purposes and provide optimized search capabilities on different parameters like users, events, time, target resources etc.		
46	The solution should have real-time session monitoring support and full audit-trail for user activities in the solution itself.		
Alerting and Integration			
47	The solution should be configurable so that events can trigger email / SMS alerts, run specific programs, and communicate with trouble ticketing applications like Saphire, other security frameworks.		
48	The solution should be capable of alerting on actions such as password requests and check-outs, password changes, failed password change jobs, console and web application activities etc. and attempts of access violations (running elevated/ higher privilege commands, modifying password/ user files, adding users to privileged groups etc.)		
49	Ability to integrate with vulnerability management solutions for deep, authenticated scans (e.g. Indus Guard, Qualys Guard, Rapid 7 etc.) i.e. should be able to provide credentials to these scanning applications during run-time.		
50	The solution should be able to provide simple methods for integrations that are not provided out-of-the-box with minimum		

	effort.		
Compliance Reports			
51	The solution should provide pre-configured reports to monitor compliance with regulatory mandates such as IRDAI, IT Act 2000, Cyber Law etc. It should also provide screen-based templates/capabilities to create/generate custom reports without writing codes.		
52	The solution should not act as a single point of failure for privilege access to systems and it should be possible to recover passwords during outages.		

B. SIEM

B. SIEM			
Sr. No	**Functional Requirements (minimum)**	**Compliance**	**Remarks (Yes/No)**
General			
1	The Solution should be an appliance based with a clear physical or logical separation of the collection module, logging module and correlation module. OEM should confirm all the appliances are sized for sustained 20,000 EPS.		
2	The solution should support log collection, correlation and alerts for the number of devices mentioned in scope.		
3	The log collection engine should have high availability without depending on third party solution. Logging and correlation modules should be proposed in standalone.		
4	The solution should have connectors to support the listed devices/ applications wherever required the vendor should develop customized connectors at no extra cost		
Log Collection and Management			
5	All logs should be Authenticated (time-stamped) encrypted and compressed before transmission		
6	The solution should be able to continue to collect log data during database backup, de-fragmentation and other management scenarios, without any disruption to service		
7	The solution should support log collection from all operating systems and their versions including but not limited to Windows, AIX, Unix, Linux, Solaris servers, HP Unix etc.		
8	In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention, deletion, synchronization with SIEM database should be automatic but it should be possible to control the same manually. Retention period that must be facilitated at the collector in case of connection to SIEM management is lost shall be at least 15 days.		

9	The solution shall allow bandwidth management, rate limiting, at the log collector level.		
10	The solution should ensure that the overall load on the network bandwidth at DC, WAN level is minimal		
11	The solution should provide time based and forward feature at each log collection point		
12	The solution management login should have strict password policy including password expiry, notification prior to password expiry, password history count.		
13	It should be possible to store the event data in its original format in the central log storage		
14	The data archival should be configured to store information in tamper proof format and should comply with all the relevant regulations.		
15	SIEM should provide backup mechanism for both configuration and data		
16	The system shall be able to capture all details in raw log, events and alerts and normalize them into a standard format for easy comprehension.		
17	It should be feasible to extract raw logs from the SIEM and transfer to other systems as and when required.		
18	Should support the following log collection protocols: Syslog over UDP / TCP, RDEP, agent-less WMI, SDEE, SCP, ODBC, FTP, LEA, Windows Event Logging Protocol, Netflow (v5, v7, and v9), sflow and jflow at a minimum.		
19	The solution should be able to collect and process raw logs in real-time from any IP Device including Networking devices (router/ switches/ voice gateway etc.), Security devices (IDS/IPS, AV, Patch Management, Firewall/DB Security solutions etc.), Operating systems(Windows 2003 / 2008, Unix, HP Unix, Linux, AIX, etc.), Mainframe(z/196), Virtualization platforms, Databases (Oracle, MSSQL, MySQL, DB2, Post-Gres etc.), Storage systems, and Enterprise Management systems etc.		
20	The solution should prevent tampering of any type of logs and log any attempts to tamper logs		
	Correlation		
21	SIEM must allow the creation of an unlimited number of new correlation rules		
22	Solution should be able to perform the following correlations (but not limited to): Rule based, Vulnerability based, Statistical based, Historical based, Heuristics based, Behavioural based etc.		
23	The system/solution should have the ability to correlate all the fields in a log		
24	The solution should be able to parse and correlate multi line logs		

25	Ability to gather information on real time threats and zero day attacks issued by anti-virus or IDS/ IPS vendors or audit logs and add this information as intelligence feed in to the SIEM solution via patches or live feeds		
26	The solution should allow a wizard based interface for rule creation. The solution should support logical operations and nested rules for creation of complex rules		
27	The central correlation engine database should be updated with real time security intelligence updates from OEM		
	Dashboard and Reporting		
28	The dashboard should be in the form of a unified portal that can show correlated alerts/ events from multiple disparate sources such as security devices, network devices, enterprise management systems, servers, applications, databases, etc.		
29	Events should be presented in a manner that is independent of device specific syntax and easy to understand for all users		
30	The solution should be able to integrate with external Asset Management DB to use asset values in security incident prioritizing process		
31	It should be possible to categorize events while archiving like events for network devices, antivirus, servers etc.		
32	Any failures of the event collection infrastructure must be detected. The device Health monitoring must include the ability to validate that original event sources are still sending events		
33	The solution should generate the following reports (but not restricted to): User activity reports, Configuration change reports, Incident tracking report, Attack source reports etc. In addition, the solution should have a reporting writing tool for development of any ad-hoc reports.		
34	The Dashboard design for the solution should be editable on an ad-hoc basis as per the individual user need		
35	The system should display all real time events. The solution should have drill down functionality to view individual events from the dashboard		
36	The solution should allow applying filters and sorting to query results.		
37	The solution should allow creating and saving of ad hoc log queries on archived and retained logs. These queries should be able to use standard syntax such as wildcards and regular expressions.		
38	SIEM should provide mechanism to map usernames, user IDs or any other values which uniquely define users with real life user information, like first and last name, job position, etc		
39	The solution should allow for qualification of security events and incidents for reporting purpose. The solution should be able to generate periodic reports (weekly, monthly basis) for such qualified security events/ incidents.		

40	Should provide summary of log stoppage alerts and automatic suppression of alerts.		
41	Should generate e-mail and SMS notifications for all critical/high risk alerts triggered from SIEM		
42	The solution should have multiple Visualization options including dial views, vertical and horizontal bar charts, text lists, pie charts, case management views etc.		
43	Dashboard should display asset list and capture details including name, location, owner, value, business unit, IP address, platform details		
44	Solution must be able to prioritize threats based on historical risk calculations		
45	Dashboard should have reporting for consolidated relevant compliance across all major standards and regulatory requirements from day one. This includes ISO 27001, IRDAI regulations, IT ACT, PCI DSS standards etc. OEM to mention if customization is required.		
46	Dashboard should support different views relevant for different stake holders including top management, operations team, Information Security Department		
47	Dashboard should support export of data to multiple formats including CSV, XML, Excel, PDF, word formats.		
48	Dashboard views should be customizable as per user rights and access to individual components of the application.		
49	Administrators should be able to view correlated events, real-time raw logs and historical events through the dashboard.		
50	Senior Management should be able to view compliance to SLA for all SOC operations		
51	The system should permit setting up geographical maps/images on real time dashboards to identify impacted areas and sources of alerts.		
52	Correlations must support: Single events, Event rates, Events sequence, Deviations from baseline. The solution should be generating an alarm when the event rate exceeds a given volume.		
53	Log collection solution should have an option to filter or choose logs at collection layer to govern flexibility to forward security related events and filter.		
Event and Incident Management			
54	The system should identify the originating system and user details while capturing event data.		
55	It should be possible to automatically create incidents and track their closure		
56	The solution should offer a means of escalating alerts between various users of the solution, such that if alerts are not acknowledged in a predetermined timeframe, that alert is escalated to ensure it is investigated.		
Storage			

57	The vendor should provide for adequate storage to meet the EPS and retention requirements. SI shall be responsible for upgrade of the storage to meet the requirements as above at no additional cost. The SI should provide adequate justification for the storage size proposed as part of the response.		
58	The solution should be able to store both normalized and RAW logs		
59	The platform should provide tiered storage for the online, archival, and backup and restoration of event log information.		
60	The Tier I and II storage should have the capability to authenticate logs on the basis of time, integrity and Origin		
61	The storage solution should have the capability to encrypt/hash the logs in storage		
62	System should have capacity to maintain the logs for 90 days online and 09 months older logs should be archived on Storage as required. UIIC will retrieve the 06 years logs on tapes to maintain the logs retention period of 07 Years.		
63	Solution should be capable of retrieving the archived logs for analysis, correlation and reporting purpose automatically.		
64	Should be able to part and filter logs before storage based on type of logs; date etc.		
65	Solution should be capable to replicate logs in Synchronous / Asynchronous mode.		
66	It should be possible to define purging and retention rules for log storage.		
67	The solution should come with built-in functionality for archiving data.		
Integration			
68	Receive database alerts from DAM		
69	Integrate with NBA, IPS, IDS, Firewall, Proxy etc. to identify network security issues		
70	Integrate with DLP solutions to identify misuse of sensitive information		
71	Integrate with PIM and other Directory solution to relate security events to user activities		
72	Should be able to integrate with physical access control systems.		
73	Integrate with existing helpdesk/ incident management tools		
74	Should be able to integrate with backup solution for performing backup of the SIEM.		
75	Should be able to integrate with all 10 Applications (Web Based Application; Insurance Application, SAP, HR) as mentioned in the RFP, during the contract period we may procure additional		

	applications/solutions /devices which is to be integrated with the SIEM Solution at no additional cost.		
76	Connector Development tool/SDK availability for developing collection mechanism for home-grown or any other unsupported applications		
77	The system should have out of the box rules for listed IDS/IPS, firewalls routers, switches, VPN devices, antivirus, operating systems, Databases and standard applications etc.		
Availability			
78	The SI should prepare a DR plan for switch over in case the DC operations are down		
79	The solution should have high availability feature built in. There should be an automated switch over to secondary SIEM in case of failure on the primary SIEM. No performance degradation is permissible in case of failure.		
80	The storage solution should have adequate redundancy for handling disk failures		
Scalability			
81	The solution should be scalable as per future roadmap for expansion		
82	Solution should support ingestion of both STIX and TAXII feeds for IOC ingestion.		
83	The solution should support creation of incident management workflows to track incident from creation to closure, provide reports on pending incidents, permit upload of related evidences such as screenshots etc.		
84	The system should receive feeds from a threat intelligence repository maintained by the OEM which consists of inputs from various threat sources and security devices across the globe.		

C. <u>DDoS</u>

C. DDoS			
Sr. No	**Functional Requirements (minimum)**	**Compliance**	**Remarks (Yes/No)**
Hardware and Performance			
1	DDoS solution should be a dedicated hardware appliance and not a licensed feature on Firewall or Load Balancer Appliance or Proxy Based Architecture or a VM based solution installed on a server machine.		
2	Device should have at least 6 x 1G copper Interfaces		
3	Should have at least 2 X 10G SFP+ interfaces		
4	System should have inspection throughput of 500Mbps and scalable to 2 Gbps without additional hardware.		

5	Proposed device should have the capacity to mitigate at least 2 times of inspected throughput as asked. This value should not be clubbed with inspected throughput / clean throughput as defined above		
6	Should support latency less than 70 microseconds and should be clearly documented in the data sheet		
7	System should have High performance ASIC-based DoS-mitigation engine that ensures that attack mitigation does not affect normal traffic processing and Maximum DDoS Flood Attack Prevention Rate up to at least 5 Million PPS		
8	SSL attack prevention Module/appliance System should Mitigate encrypted attacks and should have at least capacity of 18000 SSL CPS with 2048 bit Key		
9	In inline mode, system must not modify MAC or IP addresses of passed frames		
10	The device should have dual power supply.		
11	System should Fail-Open or should bypass the traffic in case of Hardware failure internally or Externally using Bypass Switch		
12	System should support Multiple Segment protection		
Generic Features			
13	System should support In-Line, SPAN Port, Out-of-Path deployment modes from day 1		
14	System should support following environments:		
14.1	Symmetric		
14.2	Asymmetric Ingress		
14.3	Asymmetric Mesh		
15	Solution should be transparent to control protocol like MPLS and 802.1 Q tagged VLAN environment. Also, it should transparent to L2TP, GRE, IP in IP traffic.		
16	The system should be transparent to 'logical link bundle' protocols like LACP		
17	Solution Should detect IPv6 Attacks		
18	Solution should mitigate IPv6 Attacks		
19	The DDoS detection capability of the solution must not be impacted by asymmetric traffic routing.		
20	Should detect and Mitigate attacks at Layer 3 to Layer 7		
21	Should support standard network MTU.		
22	The system must allow protection parameters to be changed while a protection is running. Such change must not cause traffic interruption		
Security / DDoS Feature			
23	System should Protect from multiple attack vectors on different layers at the same time with combination of Network, Application, and Server side attacks		
24	Solution should provide protection for volumetric/Protocol and Application layer based DDoS attacks		

25	Inspection and prevention is to be done in same hardware		
26	The system must have an updated threat feed that describes new malicious traffic (botnets, phishing, etc...).		
27	The system should be capable to mitigate and detect both inbound and outbound traffic.		
28	Solution should provide real time Detection and protection from unknown Network DDoS attacks.		
29	System should have mitigation mechanism to protect against zero-day DoS and DDoS attacks without manual intervention.		
30	System should support horizontal and vertical port scanning behavioural protection		
31	System supports behavioural-based application-layer HTTP DDoS protection		
32	System supports DNS application behavioural analysis DDoS protection		
33	System must be able to detect and block SYN Flood attacks and should support different mechanism:		
33.1	SYN Protection - Transparent Proxy/out of sequence		
33.2	SYN Protection - Safe Reset		
33.3	SYN Protection /TCP Reset.		
34	System must be able to detect and block HTTP GET Flood and should support mechanisms to avoid False Positives		
35	Should support following HTTP flood Mechanism:		
35.1	High Connection Rate		
35.2	High rate GET to page		
35.3	High rate POST to page		
35.4	DDoS device should support for Burst Attack Mitigation and signature generation based on behaviour of Attack.		
35.5	DDoS Device should support for Both Rate limiting and Behavioural Analysis.		
36	System should detect and Mitigate different categories of Network Attacks:		
36.1	High rate SYN request overall		
36.2	High rate ACK		
36.3	High rate SYN-ACK		
36.4	Push ACK Flood		
36.5	Ping Flood		
36.6	Response/Reply/Unreachable Flood		
37	System should provide zero-day attack protection based on learning baseline / behavioural analysis of normal traffic, zero-day attacks are identified by deviation from normal behaviour.		
38	System provides behavioural-DoS protection using signatures Generation		

39	System should Protect from Brute Force and dictionary attacks.		
40	System must be able to detect and block Zombie Floods		
41	System must be able to detect and block ICMP, DNS Floods		
42	The system must be able to block invalid packets including checks for :Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Bad TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped		
43	Should detect and Mitigate from Low/Slow scanning attacks		
44	should detect and mitigate from Proxy & volumetric Scanning		
45	System Should support dedicated DNS protection from DDoS		
46	System should support suspension of traffic/ blacklisting from offending source based on a signature/attack detection		
47	System should support user customizable and definable filter		
48	system should support malware propagation attacks		
49	System should support anti-evasion mechanisms		
50	System should support Intrusion Prevention from Known Attacks either on the appliance or through external appliance		
51	System should have capability to allow custom signature creation		
52	System should protect from DDoS attacks behind a CDN by surgically blocking the real source IP address		
Protection against Encrypted Attacks			
53	System should have out-of-path / on device SSL inspection from same vendor as of DDoS solution		
54	Proposed Solution should Protect against SSL & TLS-encrypted Attacks with a separate SSL Decryption module on device / out of Path		
55	Proposed Solution should provide protection for known attack tools that attack vulnerabilities in the SSL layer itself with a separate SSL Decryption module on device / out of Path		
56	Proposed Solution should detect SSL encrypted attacks at Key size 2K without any hardware changes and should be defined in the technical document provided.		
High detection and mitigation accuracy			
57	System should support Challenge-response (Layers 4 to 7) mechanisms without Scripts		
58	System should support HTTP Challenge Response authentication without Scripts		

59	System should support Polymorphic Challenge-Response mechanism without scripts		
60	System should support DNS Challenge Response authentication : Passive Challenge, Active challenge Both without scripts		
Integration Capabilities			
61	System should have capability to integrate with SIEM solution		
62	Should have ready API for SDN environment integration/ Anti-DDoS system for attack mitigation in custom portal		
Cloud DDoS Services			
63	Cloud Scrubbing should be from same OEM as on premise device		
64	Cloud Scrubbing should take / Accept Signalling from On-prem Device		
65	The Signalling should include Attack footprint intelligence to ensure effective and fast mitigation		
66	Cloud Scrubbing vendor should have 4 Tbps + of scrubbing capacity		
67	Cloud Scrubbing should provide unlimited attack mitigation (no restriction based on attack traffic volume) for legitimate BW of 500 Mbps		
68	Scrubbing Center diversion based on BGP and DNS should both be supported		
69	Cloud Scrubbing Center should have following certifications:		
69.1	PCI-DSS v3.1 (Payment Card Industry Data Security Standard)		
69.2	ISO/IEC 27001:2013 (Information Security Management Systems)		
69.3	ISO/IEC 27032:2012 (Security Techniques -- Guidelines for Cybersecurity)		
69.4	ISO 28000:2007 (Specification for Security Management Systems for the Supply Chain)		
Monitoring & Management			
70	The system must support configuration via standard up to date web browsers. System user interface must be based on HTML		
71	System must support CLI access over RS-232 serial console port, SSH.		
72	The system must have a dedicated management port for Out-of-Band management		
73	Management interfaces must be separated from traffic interfaces. System management must not be possible on traffic interfaces, management interfaces must not switch traffic		
74	System must have supporting tools for central monitoring		
75	System must have concept of users / groups / roles		
76	Management certificate must be possible to change		

77	Proposed solution should have centralized management system and helps to manage, monitor, and maintain all DDoS Appliances from a centralized location.		
78	Role/User Based Access Control should be available		
79	The system must support the generation of PDF and e-mail reports		
80	Integration with RADIUS and TACACS+		
OEM Services			
81	OEM should have their own Security research team to generate signature profile targeted at DoS Tools and must be updated weekly.		
82	OEM must have Cloud Scrubbing Capability so that it can be used in future if required		
83	Post Attack Forensics Analysis and Recommendations		
84	Quoted OEM should have India TAC for local support		
85	OEM Should provide 1 day training and knowledge transfer to Department / Team		
Certification / References			
86	Device should be Common criteria certified at least EAL 3 or above		
87	Quoted OEM product should be deployed in India at least with 3 BFSI customer reference in India in last 3 years and should provide evidence of the same		
88	OEM should be present as the dedicated DDoS solution in the market for last 5 years		
89	The Solution should be deployed and used by Internet service providers for DDoS mitigation in India		

D. <u>WAF</u>

D. WAF			
Sr. No	**Functional Requirements (minimum)**	**Compliance**	**Remarks (Yes/No)**
Hardware			
1	The proposed solution should be purpose build ASIC based hardware appliance		
2	The hardware should have minimum 6X1G interfaces		
3	The hardware should have minimum 2X10G interfaces populated with SR module		
4	The solution should have at least 16 GB of memory (RAM) to support multiple WAF / Load balancing instances and scalable up to 32 GB RAM		

Architecture			
5	Solution should be virtualization ready with OEM's own hypervisor with minimum 5 virtual WAF instances from day 1 and scalable to 10 virtual WAF instances		
6	Should support WAF Virtualization such that Department can create multiple WAF / Load Balancing instances per application / Network Segment based with complete isolation, Fault Tolerance and RBAC		
7	Should support Virtualization such that department can create multiple WAF / Load balancing instances per application / Network Segment and complete flexibility to allocate throughput per instance and have separate configuration file, routing table, session table		
8	Should support Virtualization such that individual WAF instance can be rebooted independently without affecting other instance		
9	Physical resources like memory, CPU must not be shared between WAF instance, resulting in predictable performance of each virtual instance		
10	On Demand addition & removal of computer & networking resources, virtual WAF & advanced services from virtual WAF instances with no effect on other instances		
11	Proposed solution should have the support for ICSA Lab Certified WAF from day 1 on same appliance		
12	Proposed solution should be able to detect and block the OWASP top 10 attacks		
13	Proposed Solution should be IPv6 ready as on day 1		
Performance			
14	System should support 5 Gbps L7 throughput and should be scalable to 10 Gbps L7 throughput or higher with additional license		
15	System should support minimum 600K Layer 4 Connection Per second		
16	System Should support minimum 800K Layer 7 Request Per second		
17	System should support minimum of 15000 SSL CPS with 2K bit key upgradable to 18000 SSL CPS		
18	Proposed solution should support at least 8000 ECC CPS on same device		
Additional Features			
19	System should perform load balancing for Layers 4 through 7 of the Open Systems Interface (OSI) reference model with support to the IP, TCP and UDP protocols.		
20	System should have predefined Layer 7, application level health checks (HTTP, HTTPS, LDAP, SMTP, and so on) and customized Layer 7 health checks for any binary and text based protocols		
21	System should have advanced health checks with the ability to decide on the server status based on parsing the data received by the health check		
22	System should have load balancing metric such as least connection,		

	round robin, weighted, HASH, response time		
23	System should have user configurable stickiness timeout values		
24	System should have persistency based on Layer 3 and 4, Cookie (Static & Dynamic), SSL ID, XML Tag,		
25	System Should have cookie injection in relation to session persistence		
26	Should have: TLS1.2, 2048 bits SSL and Elliptical curve Ciphers support from the time of supply. SSL and ECC should run on dedicated hardware chipset and should not be software based.		
27	System should perform load balancing for Layers 4 through Layer 7 based on application content		
28	Should support SSL Re-encryption / Back end server side encryption		
29	Should have Global server Load Balancing license from Day 1 without any restriction on DNS query per second		
30	System should have support for HTTP2.0 application as well from the time of supply		
31	WAF should detect Backend Server Failure and route the traffic to available server and should have capability of Load Balancing across the multiple servers		
32	Should be able to uniquely detect and block (if required) the end user based on internal IP address, Plugins Installed in the browser type etc. instead of going with traditional IP based blocking only		
33	Should be able to provide compliance and reporting		
34	WAF Should support both Negative & Positive Security for zero-day protection.		
35	Solution should dynamically understand the Changes on the Web/Application Server		
36	Should provide Policy creation per URL and not generic policy for URL's		
37	Should support Client Certificate Based Authentication as part of technology offering		
38	System should be capable to handle IPv4 to IPv6 translation and must be IPv6 ready		
39	System should be able to monitor the performance of the application delivered from the load balancer		
40	Should Provide Application Performance Monitoring. Should Provide the Server Side, Network Side and User side latency statistics		
41	System should be able to define the SLA of the performance for the applications.		
42	System should support SSL offload - the ability to manage client-side SSL traffic by terminating incoming SSL connections and sending the request to the server in clear text		
43	System should support backend SSL encryption – terminate the SSL clients on the front-end, and open a set of SSL sessions on the back-end		
44	System should support passing client IP addresses through Secure Socket Layers (SSL)		
45	System should support SSL certificates import/export in the PEM and PKCS#12 format		

46	System should support the ability to handle all SSL client authentication tasks (request or require client certificates) normally handled by the target server.		
47	System should support hardware-based SSL acceleration		
48	System should support SHA1 and SHA2 (Secured Hashing Algorithm)		
49	System should support managing Server certificates at the Virtual Service level		
50	System should support TLS1.2 and above		
51	System should support TCP Multiplexing, TCP optimization, connection pooling, compression, caching		
52	System Should support Http 2.0 Gateway to accelerate web applications over internet/WAN		
53	Should support ICAP integration		
54	Should support authentication Gateway		
55	Proposed WAF should support for exporting logs in CSV Format.		
56	To ease out on management and forensic analysis proposed WAF should have GUI feature to filter the events from the logs		
57	Proposed WAF should have feature set to learn the application automatically whenever there is a change in application structure and should create a policy automatically for the newly learned application structure.		
58	Proposed WAF should have Feature to self-scoring for the threats		
59	Device Fingerprinting, Support for Protocols like JSON and XML		
60	WAF should have Predefined Policy and should apply automatically whenever a new application is added to ease management and maintenance.		
General Terms and Conditions			
61	The solution should be compatible with SDN/SDDC architectures like Cisco ACI, VMWare NSX, Open stack etc.		
62	Proposed solution must be deployed in at least 3 BFSI / NBFC entity in last 3 year		

E. DAM

E. DAM			
Sr. No	Functional Requirements (minimum)	Compliance	Remarks (Yes/No)
1	The solution should be Database agnostic and should support at least the following databases: Oracle 10g, 11g, 12c SQL Server 2008, 2012 or higher Sybase ASE 15.0.3 or Higher MySQL IBM DB2		
2	The solution should support on the following OS platforms at least: IBM AIX 6.1 or Higher Microsoft Windows 2008 / 2012 all editions or Higher		

	Red Hat Enterprise Linux / Oracle Linux (latest version) HPUX 11 or Higher ORACLE SOLARIS 10 & 11 or Higher		
3	Solution does not require changes in the database application (e.g. turning audit or trace on)		
4	Solution should be a non-intrusive agent installed on the server. The agent should read the data from shared memory		
5	Solution should protect it-self from tampering and attacks		
6	Solution allows easy translation of actual database activity into monitoring / audit policy direct from alerts.		
7	Solution should be capable of capturing the alerts which will include the following metadata: Originating IP Address DB User OS User Full SQL Statement Accessed tables Application Name Module Name Host Name/Terminal name		
8	Command Type The solution should be capable of sending alerts to external applications at least through: via e-mail via syslog via SNMP traps		
9	Solution should easily integrate with SIEM and other management products		
10	Solution should be capable of monitoring of all database activities and protect against insiders with privileged access		
11	Solution should offer granular monitoring of database transactions with real-time alerts and prevention of breaches		
12	Solution should offer granular monitoring of queries, objects and stored procedures with real- time alerts and prevention of breaches		
13	Solution should provide protection against newly discovered database vulnerabilities, providing immediate protection with no DBMS downtime and without having to update the patch itself.		
14	Solution should offer flexible audit and reporting capabilities.		
15	Solution should provide multiple user roles that facilitate separation of duties		
16	Solution should capable of monitoring and alerting unauthorized access to sensitive data on the Database, like credit card tables etc.		
17	Solution should have the ability to independently monitor and audit all database activities, including administrator's activity and select transactions.		
18	Solution should record all SQL transactions: DML, DDL, DCL and SELECTS and should have the ability to store this activity securely outside the database		

19	Solution should have the ability to enforce separation of duties on Database Administrators. Auditing should include monitoring of DBA activity and solutions should prevent DBA manipulation or tampering with logs or recorded activity.		
20	Solution should have the ability to generate alert on policy violations and provide real time monitoring and rule-based alerting.		
21	Solution should have the ability to ensure that a service account only accesses a database from a defined source IP and only runs a narrow group of authorized queries		
22	Solution should capture and report on SELECT statements made on Databases		
23	Solution should report on detailed SQL, including the source of the request, the actual SQL commands, the database user name, when the request was sent and what database objects the command was issued against.		
24	Solution should report on database access including logins, client IP, server IP and source program information.		
25	Solution should track execution of stored procedures, including who executed a procedure, name of the procedure and when, which tables were accessed as a result		
26	Solution should track and audit administrative commands such as GRANT		
27	Solution should track and report all failed logins.		
28	Solution should support creation of specific rules on observed events, sending SMTP alerts when the rules are violated.		
29	Solution should Capture and report on non- administrators executing DDL.		
30	Solution should support architecture where application has pooled connections, the user name should be monitored.		
31	The solution deployed should not require any change in the DBMS binaries		
32	The agent should not demand for restart of the database while installing or while upgrading or while uninstalling the solution		
33	Solution should be able to monitor inter and intra DB activities and attacks		
34	Solution should be able to monitor activities done by administrator or any DB admin sitting directly on the database server console		
35	The solution should have a single console to manage and monitor Database Activity monitoring (DAM) and the vulnerabilities inside the database		
36	Solution should be capable of detecting weak passwords		
37	Solution Application comes with predefined reports, allows for customizing and Ad-hoc reports		
38	The solution should provide the Insurance sector relevant module and any others(Specify)		

ANNEXURE 11 - RESTRICTION OF BIDDERS FROM COUNTRIES SHARING BORDER WITH INDIA

< To be submitted in the Bidder's & OEM's letter head along with eligibility criteria >

Ref. No:
To

The Deputy General Manager
Information Technology Department
United India Insurance Company Limited
Head Office, NALANDA, #19, 4th Lane,
Nungambakkam High Road,
Chennai – 600034

Subject: Offer for RFP Ref. No. 000100/HO IT/RFP/138/2020-21 "RFP for Supply, Installation, Implementation, Integration, Maintenance and Support of Security System"

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 this bidder/OEM is not from such a country or, if from such a country, has been registered with the competent authority, I certify that this bidder fulfills 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 12 - LOCATIONS

For the purpose of solution/equipment implementation, the location of different sites is as follows:

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.

ANNEXURE 13 - 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]

Ref. 000100/HO IT/RFP/138/2020-21 – "TENDER FOR PROPOSAL (RFP) FOR SUPPLY, INSTALLATION, IMPLEMENTATION, INTEGRATION, MAINTENANCE AND SUPPORT OF SECURITY SYSTEM"

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 ₹ 50,00,000/- (Rupees Fifty 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 has not supplied/is not supplying similar products /systems or subsystems at a price lower than that offered in the present bid in respect of any other Ministry/Department of the Government of India or PSU and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very 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.

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 14 - EXISTING SECURITY EQUIPMENT AT DC & DR

To be considered for buy back

DC Network Assets

S#	Equipment @ DC : Make and Model	Qty
1	Fortigate 1101E	2
2	Fortimanager	1
3	Fortianalyzer	1
4	FortiSandbox 1000F	2
5	Cisco - ASA Firewall 5585	2
6	Cisco - VPN ASA 5585	1

DR Network Assets

S#	Equipment @ DR : Make and Model	Qty
1	Fortigate 1101E	2
2	Fortimanager	1
3	Fortianalyzer	1
4	FortiSandbox 1000F	2

ANNEXURE 15 - PREBID QUERY FORMAT

Ref. 000100/HO IT/RFP/138/2020-21 "TENDER FOR SUPPLY, INSTALLATION, IMPLEMENTATION, INTEGRATION, MAINTENANCE AND SUPPORT OF SECURITY SYSTEM."

Date:

Dear Sir,

Subject: Queries w.r.t. Ref. 000100/HO IT/RFP/138/2020-21 **for** "TENDER FOR SUPPLY, INSTALLATION, IMPLEMENTATION, INTEGRATION, MAINTENANCE AND SUPPORT OF SECURITY SYSTEM.**"**

S.No	Page#	Point / Section	Existing Clause	Query
1.				
2.				
3.				
4.				
5.				
6.				
7.				

ANNEXURE 16 - BID SUBMISSION CHECK LIST – FOR BIDDERS

S#	Document	Attached (Yes/No)	Page#
ELIGIBILITY CRITERIA ANALYSIS (Online Submission)			
1	Tender Fee remittance details.		
2	Proof of Earnest Money Deposit (EMD) amount deposited in UIIC Account / Bank Guarantee for EMD		
3	Pre-Contract Integrity Pact as per ANNEXURE 13 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		
12	Restriction of Bidders from countries sharing border with India as per ANNEXURE 13		
13	Physically Sign the RFP document and attach the scanned copy.		
TECHNICAL BID DOCUMENTS (Online Submission)			
1	Compliance Statement for the prescribed Technical specifications as per ANNEXURE. Along with all supporting documents as detailed in ANNEXURE 10.		
2	Technical Documentations (if any)		
3	Data Sheet of the quoted models		
COMMERCIAL BID DOCUMENTS (Online Submission)			
1	Commercial Bid as per ANNEXURE 7		

END OF RFP