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

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

CORRIGENDUM-4

UNITED INDIA INSURANCE CO. LTD
INFORMATION TECHNOLOGY DEPARTMENT
NALANDA
19,4th Lane
Uthamar Gandhi Salai
(Nungambakkam High Road)
Chennai – 600034
CIN : U93090TN1938GOI000108

TABLE OF CONTENTS

1. PRE-BID QUERIES & REPLIES

UNITED INDIA INSURANCE COMPANY LIMITED
HEAD OFFICE, I.T. DEPARTMENT, CHENNAI - 600014

PRE-BID CLARIFICATIONS

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

This is further to our tender notification and based on the pre bid queries received over email, we confirm the below corrigendum / amendments, for the tender ref. no. 000100/HO IT/RFP/138/2020-21 DATED. 13.08.2020 towards supply, installation, implementation, integration, maintenance and support of security system

Sr. No.	Page#	Point/Section	Existing Clause	Query	REPLY
1	7	2.4 ELIGIBILITY CRITERIA FOR BIDDERs/OEMs Point 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.	Request Dept. to kindly revise the clause as below : "The Bidder should be ISO 9000/9001, ISO 20000 or ISO27001 or IEC 27001 or Cmmi Level 3 certification holder company,with certifications valid at the time of bid submission."	As per RFP
2	8	Sec 2.4, Page 8	ELIGIBILITY CRITERIA FOR BIDDERs/OEMs 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".	We do hereby declare and affirm, to the best of our knowledge, 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".	As per RFP
3	8	2.4 (g)	Bidder should be providing SIEM Solution to minimum 2 BFSI customers in India	Request the department to rephrase the clause as "The bidder should be currently in the service of providing Security Operation Centre (SOC) and facility management services for Security solutions including at least two Government BFSI customers in India with 1000 offices / Branches." UIIC has estimated to have 20,000 EPS Licences for the current requirement. Since, SIEM is one of the critical solutions as per the scope, it is highly recommended to have Pre-qualifying criteria set for the bidder who have prior experience in Government BFSI and bidder should have implemented equivalent or higher volume of the same. Bidder should be providing SIEM Solution to minimum 2 BFSI customers in India, requesting to consider Co Operative Banks also. Request Dept. to Kindly revise the clause as below : "Bidder should be providing SIEM/SOC Solution to minimum 2 BFSI customers in India". We request to amend to ' Bidder should be providing SIEM Solution/SOC services to minimum 1 BFSI customers in India.	As per RFP
4	8	2.4 ELIGIBILITY CRITERIA FOR BIDDERs/OEMs	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	Audit for FY 2019-20 in progress. We request you to consider the unaudited balance sheet.	As per RFP
5	8	2.4 ELIGIBILITY CRITERIA FOR BIDDERs/OEMs	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.	Audit for FY 2019-20 in progress. We request you to consider the unaudited balance sheet.	As per RFP
6	8	2.4 ELIGIBILITY CRITERIA FOR BIDDERs/OEMs Point h.	The bidder must have minimum five (5) IT Security professionals on their payroll with certification in CISA / CISSP / CISM / CEH / CCSA.	Request Dept. to kindly revise the clause as below : "The bidder/bidder's parent indian company must have minimum five (5) IT Security professionals on their payroll with certification in CISA / CISSP / CISM / CEH / CCSA."	As per RFP
7	8	Clause 2.4 - Eligibility Criteria for Bidders/OEMs	Note point no. ii - NOC service providers in UIIC are not allowed to bid for this rfp	We request you to kindly re-consider your decision. The management of UIIC links, uptime, branch network, WAN management, Patch management, Change management and IOS upgrade etc. which is a standard scope of work of NOC services provider, is not being delivered by us and hence we are not your Network Operating Centre(NOC) service providers. We are a leading Security Operations Centre (SOC) service provider as well in the BFSI segment adhering to all the benchmarking standards and helping customer achieve them.	Corrigendum Issued already
8	12	3.1 SCOPE OF WORK	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.	UIIC has embarked on a security enhancment journey, Detection and Monitoring technologies and Prevention technologies play two different roles in an organisation, hence having same OEM for both technologies does not help augment security. Hence we request SIEM which is a monitoring tool and PIM, DAM, WAF and DDoS which are prevention tools should be of different OEM's.	As Per RFP

9	12	3.1 SCOPE OF WORK - OVERVIEW	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	IS UIIC have any incident management tools or bidder need to propose any ITSM tools for the same	UIIC does not have any incident management/ITSM tool. The bidder needs to propose its ITSM tools for the same. The bidder has to provide the necessary tool for ITSM with minimum 5 user license at no additional cost to UIIC.
10	13	3.1	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.	what is the EMS, NMS and ITSM tools curently used by UIIC with which the proposed platformss to be integrated? Request to please provide clarity will customer allow the bidder to integrate the new hardware and security solutions with existing NMS for health monitoring ? Also will the proposed SOC team will get access to NMS console for monitoring the health status of the installed devices etc ? Request to please provide the Make of the NMS and ITSM required to be integrated with the proposed solution ? Please clarify will customer allow bidder to use existing UIIC ITSM to use for monitoring and resolving new incidents, tickets etc.	UIIC does not have any EMS, NMS and ITSM tools . The bidder has to provide the necessary tool for ITSM with minimum 5 user license at no additional cost to UIIC.
11	13	3.1	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).	what is the LAN backbone, is it 10 Gig copper or Fibre, Pls confirm. DC maintanence team support required to perform the cabling, hope UIIC arrange support.	LAN backbone is 10 Gig copper or Fibre along with Cat 7 cable. Any support needed to perform the cabling at DC and DR will be provided by UIIC
12	13	3.1	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.	Pls provide the name of the patching tool used under UIIC.	Bidder to apply patches for the solution proposed. If any tool needed for the same, bidder need to provide the same
13	13	3. Scope of Work 3.1 SOW Overview, 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.	Request add OEM PS cost in the commercial field. Since OEM will change separate cost to do the same. Request to please provide a commercial plaeholder for the same. Please clarify whether OEM has to do end to end implementaion or only support in reviewing the Configuration, Customization and Integration.	As per RFP
14	13	3. Scope of Work 3.1 SOW Overview , V	DC & DR and branches/offices is to be carried out as per the UIIC Policies.	Request UIIC to let the bidder know about the policy to understand and comply. Since bidder or OEM not aware or not having any visibility to UIIC policy mentioned today. which may have commercial implication during implementation to meet the UIIC policy. If UIIC not going to share the policy, request UIIC to provice commercial exclusion incase of any impact of incremental commercials to abide UIIC policy can be allowed to charge UIIC at actuals.	Details will be shared with successful bidder
15	14	3.1	xxxv. Training: 3.1 xxxiii All trainings will be arranged by the selected Bidder/OEM in UIIC's premise.	Can we do remote training or it must be at the site? Pls provide the training location. Please provide the no of participant who will be attending the training from UIIC.	All trainings will be arranged by the selected Bidder/OEM in UIIC's premise OR remotely after seeking consulation/confirmation from UIIC. No. of participant attending the training from UIIC is maximum 10 at HO, Chennai.

16	14	3. Scope of Work 3.1 SOW Overview, 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.	Since customer mentioned the Switch ports provided by UIIC, do customer mean the copper or Fiber cables mentioned are the patch cords to connect ? Please clarify ? Please clarify regarding Fiber and copper cables - our underdtanding customer will provide rack space, power, colling and switch ports. We need consoider only pacth cords from rack patch pannel to severs or infra with in the rack. Please confirm assumptions ?	**Revised:** 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. All Power strips, Power cables, Network cables, Fiber cables, patch cords (copper , fiber etc.), power cords, sockets, other components needed for mounting devices in the racks and making it functional should be brought by the bidder with no additional cost to UIIC. Further, any other components required for successful implementation of the solution are to be supplied and commissioned by the successful bidder at no additional cost to the UIIC. These cables should be factory crimped cables. Also, tagging should be done at the network devices side/SOC devices/server side and wherever applicable by the bidder. Revised additional requirement of rack is mentioned in this corrigendum
17	14	3. Scope of Work 3.1 SOW Overview, 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.	Please provide us the clarity, customer not asked for separate license for UAT enviornment, only production licesnce are asked in the RFP. Will customer buy separate UAT license from all the OEM menioned in the RFP or Are OEM need to consider additional UAT license while quoting for this project ? Does customer want UAT also in HA ? Does UAT enviorment can be with minimul license and minimal hardware infra ? Does the bidder has to quote for the UAT hardware as well or UIIC will provide UAT infra ? Please clarify whether UIIC has dedicated UAT environment or not? if Yes, can bidder use the same platform for UAT? If not, is UIIC looking from bidder to build a separate UAT infra for all mentioned solutions, apart from DC & DR.	UAT environment is not needed. Bidder needs to ensure that the upgraded patches are not impacting the solution availability. UIIC's **Revised Clause** is as follows: a. Patches have to be applied in the production environment within 15 days of release of patches by the OEM and approved by UIIC. b. All major updates/upgrades have to be applied in Production, within 30 days of release of updates/upgrades by the OEM and approved by UIIC. c. 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.
18	14	3.1 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,	Please provide the bandwidth and connectivity details for which the logs need to be fetched to a centralized location	Network Bandwidth utilisation is from 2 ISP's. The details will be shared with the successful bidder. Bidder is expected to provide bandwidth needed for the soluton proposed
19	14	XII/3.1 SCOPE OF WORK - OVERVIEW	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.	Please clarify whether the rack space, Power socket and connections will also be provided by UIIC?	Only the rack space, Power and cooling will be provided by UIIC. Power Sockets will be under the scope of bidder. Revised additional requirement of rack is mentioned in this corrigendum
20	15	3. Scope of Work 3.1 SOW Overview, xx.	All the services/solutions offered should be modular, scalable, and should be able to meet UIIC requirements during the period of contract.	Please confirm, customer already provided the volumetrics in Annexure 9 which is inclusive of the scalability. Does UIIC want any additional scalabilty or modularity other than mentioned in Annexure 9 ? Since incase of any additional sclability may have commercial impact which donot have any quantifiable line item.	The solution should be proposed based on the volumeteric requirement and should have an option of scaling without replacing the existing devices. Bidder can mention what the scalability available with the proposed solutions
21	15	3. Scope of Work 3.1 SOW Overview, 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.	Does customer ITSM will be able to Track SLA or customer want the bidder to manualy track the SLA and submit the report.	UIIC does not have ITSM tool. The bidder/OEM is responible for monitoring/track SLA and submit the reports using necessary tools.
22	15	3. Scope of Work 3.1 SOW Overview, 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.	Please confirm, customer already provided the volumetrics in Annexure 9 which is inclusive of the scalability. Does UIIC want any additional scalabilty or modularity other than mentioned in Annexure 9 ? Since incase of any additional sclability may have commercial impact which donot have any quantifiable line item. Need clarity ?	The solution should be proposed based on the volumeteric requirement and should have a option of scaling without replacing the existing devices. Bidder can mention what the scalability available with the proposed solutions
23	15	3. Scope of Work 3.1 SOW Overview, 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.	Due to Pandemic and uncertain circumtances and growing rate of infection and spread of COVID 19. We request UIIC to allow configuration and other installation support remotely. So it will help to complete the project intime. Since still state to state different lockdowns, transport, lodging and boarbing issues are there. Request customer to consider the same and provide remote installation and configuration for the project.	Implementation and Commissioning of Solutions at DC & DR can be done either on -site or remote in terms of installation and configuration for the project . It is restricted to abide by the timelines as mentioned in RFP.
24	15	3.2.1 IMPLEMENTATION & INTEGRATION	Bidder is required to integrate all the proposed tools and/or solutions with the UIIC provided ticketing tools in order to log tickets.	Please provide the UIC existing ticketing tools. Kindly share the details of the existing ticketing tool at UIIC?	UIIC does not have any ticketing tools.

25	15	XVXXIII/3.1 SCOPE OF WORK - OVERVIEW	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.	Please clarify whether the trainings needs to be delivered by bidder's own resources or from OEM? Kindly share the number of participants and batches for training? We intend to specify the number of days of training. We also presume that other bidder's personnel to conduct the training, all other logistics will be provided by UIIC to all of their participants	The trainings are to be delivered by combined involvement of both bidder & OEM. No. of participants is maximum 10. No. of days/batches is to be decider by Bidder/OEM
26	15	3.1 SCOPE OF WORK - OVERVIEW	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.	We request to modify the statement as "The Statement of work to be submitted by the shortlisted bidder should be a Nil Deviation document, any assumption, deviation or conditions quoted by the bidder anywhere in the document stands null & void." as the current solution from the bidder will be based on the RFP document which will also involve assumptions and dependancies. Post the shortlist, the bidder will perform due deligene or workshop with UIIC team and finalise the no-deviation SOW document to be part of contract. We request to modify the statement as "The Statement of work to be submitted by the shortlisted bidder should be a Nil Deviation document, any assumption, deviation or conditions quoted by the bidder anywhere in the document stands null & void." as the current solution from the bidder will be based on the RFP document which will also involve assumptions and dependancies. Post the shortlist, the bidder will perform due deligene or workshop with UIIC team and finalise the no-deviation SOW document to be part of contract.	As per RFP
27	16	3. Scope of Work 3.2.1 IMPLEMENTATION & INTEGRATIONV	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	Please clarify our understanding, since IRDA or any other framewaork has many controls, however as part this RFP, the customer asked for specific set of tools. Hope the compliance to adher these framework requirements are specific to the coverage of the tools asked in the RFP only. Incase of any additional coverage or additional tools required to fufil the scope need to be considered out of scope.	As per RFP. Also, bidder has to ensure the security solution in tandem with RFP and the compliance should be under the scope of RFP.
28	16	3. Scope of Work 3.2.1 IMPLEMENTATION & INTEGRATION,V	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.	Required Clarity, the bidder will be able to take responsibility in coordinating with other vendors to integrate with SIEM or PIM. But incase of non-compatibility, Version upgrade of existing application, or any other hardware upgrade or license upgrade which are applicable to the existing application vendor cannot be covered by the scope of bidder ? Please provide claity any additional hardware and software or infra required to sucessful implementation is under the scope of bidder is only for new proposed solutions ? or even for existing application or infra or data sources upgradation or infra or HW or SW requirements ? Bidder can confirm on the on building the interface for the existing devices or device types, existing application or application types, as it will be part of the due diligence or workshop with UIIC. For any new types of devices or applications, it will depend on the types of devices or applications. In case of custom application or devices, there will be commercial impact which will be highligted to UIIC to be considered as part of change request. Please confirm.	Integration to new solution will be done by bidder. Any change thay need on the existing application (hardware,software) will not be a part of the scope by the bidder.
29	16	3.2.1 IMPLEMENTATION & INTEGRATION	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.	Please provide the details of additional logs which need to be integrated Bidder can perform the the integration of additional log sources with SIEM solution as long it is similar types of devices or applications. In case of any custom types of devices or applications, it will have commerical impact. This will be highlighed to UIIC to be considered as part of change request. KIndly confirm.	As per RFP. Details will be shared with the successful bidder.
30	16	3.2.1 IMPLEMENTATION & INTEGRATION	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.	Bidder will be able to peform the impact assessment and solution operations as per the changes to the existing regulations followed by UIIC. In case of new policies or regulations during the project tenure, it will be mututally assessed and agreed between the bidder and UIIC before it is added as part of solution operations. In case of any commercial impact, it will be highlighed to UIIC to be considered as part of Change request. Please confirm Also Kindly share the current regulations in place at UIIC.	UIIC expects the assessment and modification of solution operations as per the policies/standards/guidelines/regulation /RFP is to be done by bidder to be configured at no additional cost to UIIC. However, in future if hardware needs upgrade it will be mutually agreed with UIIC.
31	16	3.2.1 IMPLEMENTATION & INTEGRATION	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	Bidder can confirm on the on the integration of the existing devices or device types, existing application or application types for integration with SIEM solution, as it will be part of the due diligence or workshop with UIIC. For any new types of devices or applications, it will depend on the types of devices or applications. In case of custom application or devices, there will be commercial impact which will be highligted to UIIC to be considered as part of change request. Please confirm.	As per RFP
32	17	3. Scope of Work 3.2.1 IMPLEMENTATION & INTEGRATION, 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.	Need clarity on the clause. Not able to understand the expectation from customer.	**Revised:** The bidder should note that the production (DC), DR(failover) should be physically separated. UIIC does not need non-production environment (UAT/Pre-production)
33	17	3. Scope of Work 3.2.1 IMPLEMENTATION & INTEGRATION, 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.	Request to please clarity our understanding. UIIC want only dedicated Project Manager on site. Remaning Solution Architect and Security Expert resource are on-demand and need basis, can support the Project manager and project team remotely as well.	Dedicated Project Manager. It cant be only remote. UIIC will not provide people for remote access and bidder should get approval every time access is needed. Providing access will be decided by UIIC. Bidder is responsible for any security incident or downtime caused due to remote support and Penalty of 1% of contract value will be levied for any incident caused

34	17	4	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.	In public sector undertakings (PSU), there are no available guidelines which prevents bidders from participating in RFP process either for NOC or SOC service provider in event a bidder happens to be existing service provider for any such services. There are available examples in insurance sectors where there is common NOC & SOC service provider. We request that clause restricting partcipation of incumbent vendors be removed.	Corrigendum Issued already
35	18	3.2.2 MEASURE & MANAGE FUNCTION	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.	Request clarity, Will customer provide the UAT license and infra seperately to the bidder for testing ?.	As Per RFP. UAT is not needed.
36	18	3.2.2 MEASURE & MANAGE FUNCTION	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. 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.	Please clairfy our understand. UIIC will provide the required infra for the helpdesk team, like PC, Desk phone, seating, toll free numbers if required etc access to internet etc. Please clarify whether UIIC is looking for a separate helpdesk team apart from SoC team (mentioned in Annexure 7 - C. Resource table). Please clarifi whether UIIC will be providing space, phone, desktop and other facilities like EMS licenses to the helpdesk team.	UIIC will provide the required infra for the helpdesk team, like PC, Desk phone, seating, toll free numbers if required etc access to internet etc. UIIC is not looking for a separate helpdesk team apart from SoC team (mentioned in Annexure 7 - C. Resource table).
37	18	3.2 iii	Manage Services Resources should have at least 3 years of relevant experience in providing the Operation & Maintenance Services for Security solutions.	Whether bidder can proposed hybrid model for Security Monitoring, or UIIC is expecting dedicated onsite resources. The number of resources mentioned in the RFP is not sufficient to manage the 24x7 SOC operations. The purpose of building the SIEM and SOC may not be achieved in case it is not managed 24x7 and has minimum number of resources. We request UIIC to relook into the resources and provide uniform sizing for all the bidders, which will be optimal for managing the SOC operations as well as security device management.	UIIC is seeking for dedicated onsite resources. The number of resources mentioned in the RFP is kept at minimum. The bidder is free to depute additional resources 'on-need basis' with no addiitonal cost to UIIC.
38	18	V/3.2.2 MEASURE & MANAGE FUNCTION	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	Please clarify whether you are refering to dedicated steady state project manager or bidder to factor one more additional offiste project manager here.	UIIC refers to a dedicated project manager solely allocated for this project. UIIC needs single point of contact.
39	18	VII/3.2.2 MEASURE & MANAGE FUNCTION	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.	Please clarify whether UIIC is looking for a separate helpdesk team apart from SoC team (mentioned in Annexure 7 - C. Resource table). If UIIC is looking for a dedicated helpdesk team then what is the minimum resource count to be deployed who will provide the required tools for them to operate?	No separate helpdesk team. The helpdesk team will be within the same SOC team.
40	20	XVIII/3.2.2 MEASURE & MANAGE FUNCTION	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)	Please clarify whether this will be a separate team then helpdesk? The number of resources mentioned here is not sufficient to manage the services 24x7, which will impact the overall objective of implementing the solution. To have a uniform sizing for all bidders, we request UIIC to revise the resources sizing as per minimum requirement. Kindly revise.	There wont be a separate team for helpdesk. The number of resources mentioned in the RFP is kept at minimum. Bidder is free to depute additional resources 'on-need basis' with no additional cost to UIIC
41	20	XX/3.2.2 MEASURE & MANAGE FUNCTION	d. Bidder shall create the knowledge repository and shall provide UIIC Officials access to all the repository prepared for UIIC.	Please clarify whether UIIC will provide internal share folder or storage space to create knowledgebase?	Storage space of 50Gb will be provided by UIIC. Bidder to factor more if needed
42	21	3.2.2 MEASURE & MANAGE FUNCTION	Bidder to take corrective actions in order to resolve any security related issue including Malware attacks, Phishing attacks etc. occurring in UIIC.	Bidder will responsible for resolution of security related issues including Malware attacks, Phishing attacks etc. for the scope of technologies in the RFP. In case of existing tools or applications, the respective vendors will perform the remediation or resolution. Kindly confirm	Bidder will responsible for resolution of security related issues including Malware attacks, Phishing attacks etc. for the scope of technologies in the RFP. In case of existing tools or applications, the respective vendors will perform the remediation or resolution.
43	23	3.2.4.2	DDoS should support application layer	Then certificate offloading to be done, whether current certificate are supported by the DDoS solution or not to be considered.	As per RFP
44	23	3.2.4.2	DDoS Attacks over Internet links	this can be achieved using layered approach (Wherein ISP should have the DDoS protection capabilities. If complete internet pipe is chocked then onprime will not have control hence layered approach must be there.	RFP has Cloud scrubbing section
45	23	3.2.4.2	DDoS must be supported for services hosted in internet	We need to clear here, like internet facing services which are hosted in DC & DR.	All internet facing services are hosted in DC & DR
46	23	3.2.4.2	Solution should identify the root cause	Its very difficult in most of the cases as it requires Deep analysis to find out the root cause	As per RFP. SOC should provide analysis

47	23	3.2.4.2	Behaviour of the application visitors.	Need more clarity	It has been clearly mentioned in RFP to monitor the behavior of the application visitors (in terms of attacker/user/application)
48	23	3.2.4.2	Solution Integration	what are other security solution	SIEM integration . Pls refer the scope of work
49	23	3.2.4.2		Need Number of web applications and the certificate details to ensure the right WAF solution.	These will be shared with the successful bidder
50	23	3.2.4.2		Need Each application concurrent session requirement	Will be shared with successful bidder. Technical requirement for the solution is mentioned in RFP
51	23	3.2.4.2		Is there any latency sensitive applications? That to be taken care some time multi layer approach might create impact on the latency sensitive application.	Yes
52	24	3.2.4.1	DISTRIBUTED DENIAL OF SERVICE (DDoS) 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	Pls eloborate on what L2 (Lan side DDoS attacks) attacks to be covered.	Layer 2 Attacks like Mac flooding
53	25	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM), Point v	Develop parsing rules for non-standard logs	Request UIIC to mention No. of device needs custom parser creation to arrive efforts estimation.	As per RFP. UIIC cannot forsee the kind of attack in future. No. of devices is not known.
54	25	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)/ STORAGE	General Clarification	Would UIIC's log sources for SIEM be at DC and DR only or at other locations also? If Yes then how many such locations would be there and what could be the EPS volume generated from those locations?	UIIC's log sources for SIEM will be at DC and DR only.
55	26	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM), Monitoring, Point iv	The SIEM should be able to log automated tickets on Ticketing Tool based on the criticality and threshold defined.	Request UIIC to provide existing Ticketing tool details to arrive integration efforts with SIEM.	Currently, UIIC does not possess any existing Ticketing tool
56	26	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM), Storage, Point 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.	Request UIIC to confirm does post 90 days logs to be exported to TAPE or post 9 months offline logs to be exported to TAPE. Also request UIIC to mention Bare minimum storage allocation size for subject requirment to maintain uniformity across OEM. Request UIIC to confirm does post 90 days logs to be exported to TAPE or post 9 months offline logs to be exported to TAPE. Also request UIIC to mention Bare minimum storage allocation size for subject requirment to maintain uniformity across OEM. Bidder understood that, all required backup software and TAPE drives arranged by UIIC, please clarify Please Clarify whether the required TAPE libraries and drives will be provided by UIIC or bidder has to condsider?	**Revised:** 90 days of online storage, 9 months of compressed storage should be maintained by the bidder with no additional cost to UIIC (Total 1 year at any point of time i.e. 90 days online & 9 months compressed storage). Post 9 months, offline logs are to be exported to TAPE/drives. It is the responsibility of bidder to maintain offline logs beyond this 1 year period till the expiry of the contract i.e. 5 years. The required TAPE libraries/drives need's to be provided by bidder, with no additional cost to UIIC
57	26	Storage (i)	The Bidder is required to propose the solution in order to store 90 days logs (normalized Logs) online.	UIIC expecting central storage or local attached storage to appliance/servers, please clarify	It is upto bidder to go for central storage or local attached storage to appliance/servers
58	26	Storage (iii)	The bidder is responsible for automated online replication of logs (online/ archival) from DC to DR for redundancy.	UIIC expecting SAN replication, please clarify Please Clarify whether the replication tool from DC to DR will be provided by UIIC or bidder has to condsider?	Replication of logs to be done. Bidder to provide the details on how it is achieved
59	26	Storage (iv)	The solution should be capable of automatically moving the logs from online to archival drives based on the ageing of the logs.	Bidder understood that Storage auto tiering is the UIIC expectation, please clarify	Solution should have the function
60	26	3.2.4.4	**Solution Implementation:** Deploy the DAM for DC and DR locations for the in-scope databases	Need to understand different kinds of databases exist and are in scope to check the compatibility with DAM solution	Oracle
61	26	3.2.4.4.	**Solution Integration:** 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.	DAM tool will be integrate with SIEM tool and SIEM tool will provide a correlated view of threaat and vulnerabilities associated with them along with remediation mechanism. Also Which SIEM is exist in the UIIC environment.	Integration to be done with proposed SIEM
62	26	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)	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.	Bidder will integrate the additional security devices during the contract period, provided it is supported out of box by the SIEM solution. In case of any custom solution or devices, it will require vendor professional services which will have commerical impact. This will be informed to UIIC and be part of change request. Kindly confirm	Yes, any custom solution or devices if needed to be integrated has to be implemented after the consulation with UIIC
63	27	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM), Storage, Point ii	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.	Request UIIC is mention Min License to be factored for SIEM in sustained EPS mode as each OEM has different sizing parameters and considerations.	As per sizing given in volumetrc section
64	27	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)	iii. Perform log backup and archival as per UIIC's policy requirements and applicable legal/statutory requirements of Govt. of India.	Kindly share the log retention requirement for SIEM solution as per UIIC's security policies? Can bidder leverage on the existing storage solution for the log retention, instead of dedicated stoage solution for the project?	Bidder has to provide necessary tapes for the solution's proposed, with no additional cost to UIIC

65	27	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)	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.	Kindly confirm if all these regulatory guidelines are applicable for UIIC's security policies? Bidder expects UIIC to be compliant to these regulations for the existing network except for the new solution included as part of this RFP. Kindly confirm	Report related to the compliance is expected out of the box or customized
66	28	3.2.4.6	ACTIVE DIRECTORY MIGRATION	what is the current OS version? Would be the hardware provided by UIIC? How mnay total users, domains, roles and Group policies to be created?	UIIC to provide hardware for Active Directory. Total users, domains, roles and Group policies to be created by bidder/OEM based on requirement of UIIC users.
67	28	3.2.4.6 (1)	All the domain controllers will be updated to the latest version (Windows Server 2016) on a new hardware.	(i)Bidder wants to know current windows version/edition and exact count in DC and DR. Also understood that existing AD doesn't need to be upgraded and all roles should be moved to new servers and decommision old. (ii)Please clarify and also great if server sizing preference provided. Please help with current version of AD	Currently, UIIC uses Windows Server 2008 R2. Existing AD doesn't need to be upgraded and all roles should be moved to new servers and decommision old. Hardware sizing should be based on the Windows version
68	29	3.2.4.6 (1)	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)	Bidder understood that current Domain controller count per site is 2+2 in DC and DR. Should consider upgrade only in DC by using new hardware and just upgrade windows version to 2016 in DR in current server. Hence no hardware needs to be factored for DR. Please clarifty. Currently AD servers are hosted on VM or Physical Server ? Please help with current server configuration and future growth considering past experience, this will help in preapring new servers specification/configuration.	Total 6 DCs (4 primary and 2 DR). Currently, UIIC uses Windows Server 2008 R2. UIIC will provide the hardware for the same. Currently, AD servers are hosted on Physical Server . Server configuration will be shared with the successful bidder
69	29	3.2.4.6 (1)	AD integration with NTP source for Time synchronization	Bidder understood that existing Domain controllers are also integrated with external NTP source and new setup should integrate with same source, please clarify Please provide the NTP source details	Will be shared with the successful bidder
70	29	3.2.4.6 (2)	Delegation Model	Bidder understood that, delegation model other than standard, need banks support in creating any custom previlage RBAC's	Will be provided to the successful bidder
71	29	AD Migration Scope		We request UIIC team to clarify the no of forest in the current enviroment	Will be provided to the successful bidder
72	29	AD Migration Scope		We request UIIC team to provide current AD FL details	Will be provided to the successful bidder
73	29	AD Migration Scope		We request UIIC team to provide current domain controller OS details	Will be provided to the successful bidder
74	30	3.2.4.6 (4)	Application Integration with AD	Application integration carried out by app vendor and all required support will be provided from AD management team, please clarify	Any changes needed on the AD for application integration will be bidder scope
75	30	3.2.4.6 ACTIVE DIRECTORY MIGRATION / Migration Scope /3. AD Clean Up	A dedicated L2 resource with organization-wide permissions must be appointed to carry out this activity – once every 6 months	Is this over and above the FMS requirement or expected as a part of FMS.	As per RFP
76	30	3.2.4.6 ACTIVE DIRECTORY MIGRATION / Migration Scope /5. Workstation Management through AD	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.	Is creation of any new GPO is part of bidder scope ?	Yes
77	31	3.2.4.6 ACTIVE DIRECTORY MIGRATION / Migration Scope /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.	1. Please help JD or qualification criteria for L1 resource. 2. Do we need to consider L2 resources as well for DR drill management and Capacity Management as L1 resouce may not be able to handle such activties.	Bidder to provide resources as per RFP requirement
78	36	4.5	The EMD made by the bidder will be forfeited if: a) The bidder withdraws the tender after acceptance. b) The bidder withdraws the tender before the expiry of the validity period of the tender. c) The bidder violates any of the provisions of the terms and conditions of this tender specification. d) The successful bidder fails to furnish the required Performance Security within 15 days from the date of receipt of LOA (Letter of Acceptance)	The bidder requests for the following modification: "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 materially violates any of the provisions of the terms and conditions of the mutually accepted contract ~~this tender specification~~. □ The successful bidder fails to furnish the required Performance Security within 30 ~~15~~ days from the date of receipt of LOA (Letter of Acceptance)" Request UIIC to please clarify the appication of S.No b) and c)	As per RFP
79	38	Sec 4.10.1, Page 38	ACCEPTANCE OF THE SOLUTION	We propose to delete any references to subjective satisfaction of Customer wrt acceptance process and limit acceptance to meeting agreed specifications. Bidder proposes to add time frame to 2 business days within which Customer must accept/reject our services, else services shall be deemed accepted.	As per RFP

80	38	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.	The bidder requests for the following modification: "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 as mutually agreed by the parties ~~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."	As per RFP
81	39	4.1	The successful bidder shall sign the agreement within 15 days from the date of Letter of Acceptance (LOA) from UIIC.	The bidder requests for the following modification: "The successful bidder shall sign the mutually agreed agreement within 30~~15~~ days from the date of Letter of Acceptance (LOA) from UIIC."	As per RFP
82	40	**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.	Bidder requests PBG be equivalent of 10% of the annual contract value. Bidder requests PBG to only be invoked in case of material breach and that a cure period of 30 days to be given before invoking the same.	As per RFP
83	41		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.	Bidder requests that any legitimate increase in cost due to change in delivery locations be paid to the bidder	As per RFP
84	42	11	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.	The bidder requests for the following modification: "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~~.~~, provided that the Company promptly (i) provides a written notice of the claim; (ii) supplies information as requested by the bidder; and (iii) provides the bidder reasonable co-operation and allows the bidder to control the defense and settlement , including mitigation efforts. The above use or infringement thereof shall not apply to any third-party products or any non-bidder logoed product. Each party grants only the licenses and rights specified in this Agreement. No other licenses or rights (including licenses or rights under patents) are granted either directly, by implication, or otherwise. Each party shall retain ownership of its respective pre-existing intellectual property rights. Any commercially off-the shelf software supplied under this contract will be regulated solely under the standard license agreement of such software and such license will not be impacted by the terms and conditions set-forth in this Agreement."	As per RFP
85	42	12	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.	Bidder requests that there should be clip on the % increase in volume and not unlimited & The bidder requests for the following modification: "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 through the execution of a variation agreement~~without any changes in unit price of the ordered quantity~~." Request UIIC to either delete this clause or provide a cap on the additional items of bill of materials so as to enable the Bidder to submit a competitive bid.	As per RFP
86	42	13	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 bidder requests for the following modification: "Company reserves the right to change/modify locations for support of the items through the execution of a variation agreement. 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~~."	As per RFP

87	42	16	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 requests for the following modification: "The Bidder shall, at its own expense, defend and indemnify UIIC against any third party claims in respect of any damages or compensation payable as may be finally awarded by a court in consequences of any ~~accident or~~ personal injury sustained or suffered by its (Bidder's) employees or agents, or by any other third party resulting from or by any act of 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 arising from any fines or penalties imposed by a statutory or regulatory authority 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 tangible 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,~~ The above mentioned indemnities shall be applicable 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." Request UIIC to amend the clause as below as a) for performance of the services, UIIC has remedy of performance guarantee; b) use of deliverables/services will not be under of Bidder, c) Bidder's indemnities has to be carved within Clause ~~18 of this RFP/Agreement~~	As per RFP
88	42	12	12. PURCHASER'S RIGHT TO VARY QUANTITIES / REPEAT ORDER	Reques to please put a cap on the repeat orders and the prices will be agreed mutually for the repeat orders due to uncontrollable external factors determining the prices. Request UIIC to amend the clause as - OEM's to support the bidder with the price validity for a period 6 months	As per RFP
89	43	17	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 A- 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 A- 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 26, 34 and 35.	The bidder requests for the following modification: "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 A- 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 A- 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 and shall be applicable for reasons solely aplicable to the bidder. ~~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.~~ Payment of liquidated damages, if any, shall be the sole and exclusive remedy of UIIC~~Liquidated damages are applicable over and above all the penalties mentioned in clauses 26, 34 and 35.~~" Bidder requests, if it 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 value of delayed implementation deliverable (ANNEXURE 7, Table D- SOC Implementation) for every week (seven days) or part thereof of delay, up to maximum deduction of 5% of the value of delayed implementation deliverable (ANNEXURE 7, Table D- SOC Implementation) We request that LD should be applicable on value of goods / services that is delayed and not on TCO. Also request overall LD be capped to 5% of the value of goods / services delayed.	As per RFP
90	43	17	up to maximum deduction of 10% of the contract price (ANNEXURE 7, Table - Grand total)	Bidder requests that Liquidated damages only be applied on the corresponding price for HW and not on total contract price	As per RFP
91	44	Sec 17, Page 44	LIQUIDATED DAMAGES DURING DELIVERY, INSTALLATION & WARRANTY	We propose to amend clause to include additional 30 days' time period must be provided prior to levy of LD and LD must be sole and exclusive remedy wrt Bidder's failure to provide services in question by the due date. Further, both parties agree to mutually discuss LDs applicable to this deal. Also, LDs shall only apply in cases where failure is solely and directly attributable to Bidder and at no fault of Customer or other third party or occurrence of Force Majeure event.	As per RFP
92	44	16. Indemnification	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:	**Subject to Clause 18 of this RFP/Agreement,t**~~T~~he Bidder shall further indemnify UIIC against any proven loss or damage arising out of loss of data **(solely attributable to Bidder)**, 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:	As per RFP

93	44	16. Indemnification	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.	Request UIIC to limit the indemification for tangible property only & remove "etc" for clarity purpose and amend the clause as follows: The Bidder shall further indemnify UIIC against any proven loss or damage to UIIC's premises or **tangible** 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.	As per RFP
94	44	17. Liquidated Damages	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.	Request UIIC to amend this clause since Bidder shall not be penalised for the successful completion of work done within the prescribed timelines: 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 **for the undelivered portion of work** (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 **for the undelivered portion of work** (ANNEXURE 7, Table - Grand total). Once the maximum is reached, UIIC may consider termination of the contract.	As per RFP
95	44	Clause 16 - Indemnification	Indemnnity against Infringment against Patent, trademarks, copyrights, etc.	Neither party will gain by virtue of this Agreement any rights of ownership of copyrights, patents, trade secrets, trademarks or any other intellectual property rights owned by the other or any third party. We are not the manufacturer and we will not be able to transfer any IPR in relation to products, as such the warranty stipulated in Clause 13 Page 21 shall not be applicable to the Bidder. However, the Bidder shall ensure that they have the requisite license from third party before selling products to client to ensure there is no claim of infringement. All Products delivered under this Agreement are subject to the warranties provided by the OEM's or OSD's manufacturer as legally and contractually permissible for the bidder to pass onto, resell, or assign to Client. Unless otherwise specified, bidder is not the manufacturer of the Products and provides no warranty in respect of the Products. Bidder disclaims any and all warranties, whether express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose and against infringement of intellectual property rights. "	As per RFP
96	45	Sec 18, Page 45	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.	Bidder proposes replacing liability clause with following: The Bidder shall not be liable for (a) any indirect, incidental, special, consequential, exemplary or punitive damages or (b) any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, loss of data, interference with business or cost of purchasing replacement services arising out of the performance or failure to perform under the contract, whether or not caused by the acts or omissions or negligence (including gross negligence or willful misconduct) of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. NOTWITHSTANDING ANY OTHER PROVISION CONTAINED IN RFP/NDA, BIDDER'S TOTAL AGGREGATE LIABILITY FOR ALL CLAIMS ARISING OUT OF THIS RFP/NDA, SHALL BE LIMITED TO THE MOST RECENT TWELVE (12) MONTHS OF CHARGES COLLECTED BY BIDDER PURSUANT TO THE APPLICABLE PURCHASE ORDER GIVING RISE TO THE CLAIM The bidder requests for the following modification: "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 even if it has been advised of the possibility of the same.". Bidder's cumulative liability (including any indemnities) for its obligations under the contract shall not exceed 100% of annual Contract value and the bidder shall not be liable for incidental / consequential or indirect damages including loss of profit or saving, loss of goodwill, downtime costs, business interruption, diminished business value, exemplary, punitive, special or consequential Losses. Request to please limit the cumulative liability of the bidder to the invoice value of last 12 months	As per RFP
97	45	19	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.	The bidder understands that the clause hereunder refers to being declared as bankrupt or insolvent by a court of competent jurisdiction. Please confirm	As per RFP
98	45	Clause 20	Force Majeure	Please include pandemics and the governmental notifications affecting the delivery of services as well in the Force Majeure conditions	Pandemics are notified under Force Majeure by the Govt., if situation warrants

99	46	23	TERMINATION: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.	Bidder proposes to amend this clause to make it mutual and state that either party has right to terminate Agreement; notice period in case of termination for convenience is very short and should be extended to 90 calendar days. Further, Customer shall be liable to pay termination charges, mutually agreed between the parties, while exercising the right to terminate for convenience. We propose to amend this clause to make it mutual and state that either party has right to terminate Agreement; notice period in case of termination for convenience is very short and should be extended to 90 calendar days. Further, Customer shall be liable to pay termination charges, mutually agreed between the parties, while exercising the right to terminate for convenience. Bidder requests a notice period of 90 days and a lock in period Bidder requests deletion of Termination for convenience clause. Further requests, termination to be done only in case of material breach by Bidder and a cure period of 30 days to be provided. Bidder also requests that in case of non-payment of invoice by customer as per the agreed payment terms, Bidder has the right to terminate/suspention the contract after giving 30 days' notice. In case of "Termination by Convenience" Customer should pay for the remaining period as per the contract or relevant SOW as Early termination charges.	As per RFP
100	46	21	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 bidder requests for the following modification: "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 and Conciliation Act, 1996 ~~Arbitration of the Indian Council of Arbitration~~ and the award made in pursuance thereof shall be binding on the parties. A sole arbitrator shall be mutually appointed by the parties"	As per RFP
101	46	23	Termination	Bidder requests a corresponding right for termination in case of non payment by UIIC Bidder requests that bidder be paid for all the goods and services delivered till the date of termination Bidder requests a payment for any winddown charges, balance sheet charges, prepaid costs and any reverse transition costs	As per RFP
102	47	23	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.	The bidder requests for the following modification: "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 material 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. In case of such termination, Bidder shall be paid for all the goods and services delivered till the effective date of such termination" Request UIIC to terminate the contract for Bidder's material breach since for other breaches, UIIC has the remedy for liquidated damages 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 materially breaches its obligations under the tender document or the subsequent agreement/purchase order and if the material breach is not cured within 30 (Thirty) days from the date of notice.	As per RFP
103	47	24	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.	Bidder requests deletion of this clause. Please confirm.	As per RFP
104	47	25	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 bidder requests for the following modification: "The contract/agreement between the Vendor and the Purchaser will be signed in accordance with all the mutually agreed terms and conditions mentioned in this tender document and addendums/corrigendum." Request UIIC to amend this clause as few terms and conditions may have to be mutually agreed at the time of contracting stage and in parallel, UIIC may forward the contract/agreement template as a corrigendum for Bidder's reference. 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 along with mutually agreed terms and conditions at the time of final contract.	As per RFP
105	47	25	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.	The bidder requests for the following modification: "The successful bidder has to furnish the mutally agreed duly signed contract/agreement along with the security deposit/performance guarantee for UIIC's counter signature within 30 ~~15~~ days from the receipt of LOA."	As per RFP

106	47	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.	Request UIIC to provide the termination fee details and pay for all/respective portion of the services rendered till the date of termination	Payments for the services rendered till date of termination (under termination for convenience) shall be paid by UIIC
107	48	27. PROJECT TIMELINES	Installation, commissioning and Implementation 24 Weeks from the Date of Issuance of PO	Request to provide 30 Weeks from the date of issueance of PO. Because of Coronavirus, we request you to extend the timeline for delivery 12-14 weeks from PO and timeline for Installation, commissioning and Implementation to 28 weeks from the date of PO.	**Revised:**Installation, commissioning and Implementation 28 Weeks from the Date of Issuance of PO
108	49	Clause 28	Warranty and on-site maintenance	Request add - All Products delivered under this Agreement are subject to the warranties provided by the OEM's or OSD's manufacturer as legally and contractually permissible for the bidder to pass onto, resell, or assign to Client. Unless otherwise specified, bidder is not the manufacturer of the Products and provides no warranty in respect of the Products. Bidder disclaims any and all warranties, whether express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose and against infringement of intellectual property rights. "	As per RFP
109	53	29	PAYMENT TERMS :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	Bidder requests further clarity on detials of default and delays for which the payments will be withhold.	As per RFP
110	53	29	PAYMENT TERMS :FM Support(If applicable)-Payment will bemade quarterly inarrears.	Bidder requests to change it to monthly arrears. Bidder requests monthly in arrears payment Request amend the FM payment terms to monthly in arrears	As per RFP
111	53	29	Payment terms	Bidder requests clarification on the number of payment days Bidder requests that 100% of HW payment be made on delivery Bidder requests a late payment fee of 2% Per month for any delayed payment Bidder requests a right to assign to collect payments to a third party	As per RFP
112	53	29. Payment terms	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.	We reqeust you to release the payment solution wise, For example if we complete the PIM solution, UIIC shall release the payment towards the delivery and installation charges for the respective solution. Installation charges shall be paid on phasewise.	As per RFP
113	54	30.2 and 30.3	PENALTIES AND DELAYS IN BIDDER'S PERFORMANCE; DELAY IN BIDDER'S PERFORMANCE	Bidder proposes to amend clause to include additional 30 days' time period must be provided prior to levy of penalties and penalties must be sole and exclusive remedy wrt Bidder's failure to provide services in question by the due date. Further, both parties agree to mutually discuss penalties applicable to this deal. Also, penalties shall only apply in cases where failure is solely and directly attributable to Bidder and at no fault of Customer or other third party or occurrence of Force Majeure event.	As per RFP
114	54	Sec 29, Page 54	PAYMENT TERMS 1. Hardware/ Appliance- 70% on Delivery; 30% on installation. 3. Installation, Implementation & Commissioning- 100% on Ducumentation. 4. FM Support- Quarterly in arrears.	Bidder proposes to add following clause: Bidder reserves the right to charge interest@1.5% pm on delayed payments, from the due date to the date of actual payment. Bidder proposes the following payment terms: 1. Hardware/ Appliance- 100% on Delivery. 3. Installation, Implementation & Commissioning- Bidder requests the implementation fees be linked with individual milestones. 4. FM Support- Monthly in arrears. Also, bidder requests monthly in advance payments be made with 30 days from date of invoice. Request to please ammend the payment terms as 90% on Delivery and 10% on Installation.	As per RFP
115	55	Sec 30.2-30.3, Page 55	PENALTIES AND DELAYS IN BIDDER'S PERFORMANCE; DELAY IN BIDDER'S PERFORMANCE	We propose to amend clause to include additional 30 days' time period must be provided prior to levy of penalties and penalties must be sole and exclusive remedy wrt Bidder's failure to provide services in question by the due date. Further, both parties agree to mutually discuss penalties applicable to this deal. Also, penalties shall only apply in cases where failure is solely and directly attributable to Bidder and at no fault of Customer or other third party or occurrence of Force Majeure event.	As per RFP
116	55	31	The cost of the audit will be borne by UIIC.	Cost of audit should be shared by UIIC and bidder	As per RFP

117	55	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**.	Request UIIC to amend this point so that if any minor errors can be cured by the Bidder: 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 **only after a cure period of 30 days from date of event of default**: □ **Forfeiture of performance security**, □ **Imposition of liquidated damages**, □ **Termination of the contract for default**.	As per RFP
118	56	Sec 31, Page 56	INSPECTION OF RECORDS & 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.	Bidder requests that clause be amended to cover following aspects: • Bidder records wrt matters covered by this RFP shall be made available to the Customer, subject to Customer providing not less than 30 days' prior written notice to Bidder or its designees of any such audit, at any time during normal business hours, to audit, examine the relevant data. •□Such audit will be subject to Customer and auditors entering into confidentiality agreement with the Bidder and no conflict of interest. • The auditors would be permitted to submit their findings to the Customer. • The cost of the audit to be borne by the Customer. • 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/audit. • The audit shall be conducted not more than once in a calendar year and remote hands fee be applicable to the same. "Remote Hands Fee(s)" shall mean Bidder's standard rates for any facility under audit and are intended to compensate Bidder's costs for providing Customer access to Bidder's facilities and personnel during the audit. • The audit should not exceed a time duration of 4 hours (in any case should not exceed 8 hours) at any given instance. • Bidder shall not provide any information related to books of accounts/financial data. Request UIIC to amend this point as below for transparency in audit reports: Said records are subject to examination. UIIC's auditors (provided auditor is not a competitor of Bidder) 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	As per RFP
119	57	35	Service Level Agreement	The bidder requests for: a. The maximum aggregate penalty for any breach of SLA to be limited to 5%; b. Payment of SLA penalty shall be the sole and exclusive remedy of the company for failure to meet the applicable SLA; and c. SLA penalties shall be applicable for delays applicable to the bidder.	As per RFP
120	58	**35.4 SERVICE LEVEL CRITERIA**	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)	Bidder requests the penalty not be linked with Total quarterly Maintenance cost, rather requests the cost reference for SLA penalty to be linked with quarterly Manpower cost, with a maximum capping at 5% of the total quarterly FM manpower cost.	As per RFP
121	59	35.4	Service Level	Request to please clarify the formula for Quarterly Maintenance cost	The formula is mentioned in our RFP page no.59
122	64	35.4 SERVICE LEVEL CRITERIA	Security Device Management and Administration □ 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.	Modification on Penelaties as □ 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 1,000 for each default. □ For wrong rule modification in any of the security solutions will incur a penalty of INR 1,000 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 1,000 for each default.	As per RFP
123	64	Resource Deployment SLA	Penalty shall be INR 2, 00,000/- for each default beyond the agreed threshold.	We request UIIC team to amend this clause as INR. 10, 000/- for each default.	As per RFP
124	64	Resource Deployment SLA	Program Manager/Delive ry 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	We request UIIC team to amend this clause as follows "Program Manager/Delive ry Manager- Penalty shall be INR 5,000 for each week of default or part thereof Other Staff- Penalty shall be INR 1,000 for each week of default or part thereof	As per RFP
125	64	Resource Deployment SLA	Penalty shall be INR 5,000 for every 2% default or part thereof below the agreed threshold	We request UIIC team amend this clause as "Penalty shall be INR 2,000 for every 2% default or part thereof below the agreed threshold	As per RFP

126	68	MAF	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.	OEM can untake responsibility of there products and services like maintenance - warranty/AMC of the products, while OEM recommend partners/bidders based on the current knowledge, what will happen in future cant be forseen by OEM. In case the present bidder is unable to maintian the solution OEM can only recommend other qualifiy partners/bidders. Whether they will be ready to execute the future contarct esp from Bidder manpower stand point or other bidder related cost has to be addressed by bidder or the new partner, OEM can only restrict them to there scope. Please redefine this clause	As per RFP
127	70	Annexure - 4: Statement of Nil Deviations		Request UIIC to please delete this annexure as all terms and conditions may be mutually agreed between both the parties at the time of contracting stage.	As per RFP
128	71	Annnexre - 5: Bank Guarantee Format for EMD	THE CONDITIONS of this obligation are: i) If the Bidder/System Integrator withdraws his offer after issuance of letter of acceptance by UIIC; ii) If the Bidder/System Integrator withdraws his offer before the expiry of the validity period of the tender. iii) If the Bidder/System Integrator violates any of the provisions of the terms and conditions of this tender specification.	Request UIIC to please clarify S.No ii) and iii) of the CONDITIONS of this obligation.	Query not clear
129	73	Annexure 6 Sr. No. (f)	The Bidder should have implemented or have under implementation, minimum 2 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	We request you to amend to ' The Bidder should have implemented or have under implementation, minimum 2 of the below mentioned security solutions for atleast 1 BFSI Customer in india with minimum 750 offices/Branches i.PIM ii.SIEM iii.DDoS iv.WAF v.DAM The Bidder should have implemented or have under implementation, minimum 3 of the below mentioned security solutions for atleast 1 BFSI / Enterprise customer in India with minimum 250 offices / Branches - PIM / SIEM / DDoS / WAF / DAM	As per RFP
130	75	ANNEXURE 6 - ELIGIBILITY CRITERIA FORM/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	Number of BFSI branches will not be the right indication of judging the OEM capability, we request the UIIC to modify this as BFSI/ PSU/ defense organization in India or mention as minimum 10000 EPS reference customer base. We @ McAfee have been serving the lot of mission critical SIEM projects in India under PSU undertaking and request UIIC to take note of it and modify the eligibility criteria to qualify us. Otherwise UIIC will lose one of the credible SIEM player from not participating in this tender only due to this eligibility criteria.	**Revised:** For SIEM The proposed OEM solution mentioned above 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. OR 2 BFSI/ PSU/ Central Govt. Defense organization in India with a minimum of 10,000 EPS (scalable to 20,000 EPS) reference customer base. For PIM,DAM,WAF,DDoS Each of the proposed OEM solution mentioned above 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.
131	76	C. Resources :	In commercial BID format Day to Day supporting of Security tools 1.PIM 2 SIEM 3 DDoS 4 WAF 5 DAM resource is not mention only Implementation resource format are given.	Please clarify that bidder should propose the resource for day to day operation for security tools. Or not.	Yes
132	77	77 of 117; AN N EXUR E 7 - COMM ER CIAL B ID FORM AT * ALL AM OUNT S S H OUL D B E IN IN R /C. Resources	Support Executive (L1) at HO / DC for Active Directory (Mon- Fri, 9:00 - 18:00 hrs)	Please help with no./qty. of resources require.	**Revised**: Pls refer the corrigendum issued (Revised Commercial bid format - Annexure - 7) below the excel sheet
133	78	Annexure 8	Non-Disclosure Agreement	The bidder requests for the execution of the NDA on mutually acceptable terms.	As per RFP

134	83	ANNEXURE 9 - VOLUMETRIC	SIEM, EPS 10000 scalable to 20000	The proposed SIEM product should be able to handle 10,000 sustained EPS. All licenses and hardware should be sized on peak EPS. Peak EPS should be double the capacity of I.e. 20,000 sustained EPS. Request to confirm while considering the Hardware sizing to be proposed for the SIEM and corresponding storage to be proposed. Please do mention the hardware sizing required is for 10000 EPS or 20000 EPS from day 1 ? The storage required to store logs for 3 monts online and 9 months to be sized for 10K EPS and 20K EPS ? Kindly clarifiy the SIEM architechure as this point contradicts point mentioned in SIEM/General "The log collection engine should have high availability without depending on third party solution. Logging and correlation modules should be proposed in standalone".	SIEM should be proposed with 10000 sustained EPS from day one. Upgrade to 20000 EPS will be through adding license only and no change in hardware. The storage to be factored for 20000 EPS.
135	84	ANNEXURE 9 - VOLUMETRIC 5. WAF	should support 5 Gbps L7 throughput and should be scalable to 10 Gbps L7 throughput or higher with additional license	Please confirm the scalability required is 10 Gbps of L7 or please mention the throughput required inplace of higher ? Since every appliance has the CPU, RAM which has the limitation of HW. Please provide clarity the mentioned L7 through is incluse of SSL inspection ?	As per RFP. Throughput includes SSL inspection
136	84	Annexure 9->Point no 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	1. For Szing confirm do we have to consider current active core details or scablable core details. 2. Confirm on total no of databases in DC and DR 1. For Sizing please confirm, do we have to consider current active core details or scablable core details? Could you please provide us the following information in regard to the Active databases: Number of Small sized databases Number of Medium sized databases Number of Large sized databases 2. Please confirm, total no. of databases in DC and DR.	Bidder to decide. Solution should be scalable without addition commercials to UIIC
137	84	PIM (8)	The platform should be highly secured/encrypted tamper-proof for the solution and for the storage. The solution should provide webbased interface for easy access and management.	If Storage refering in the point is central, encryption also has to be enabled in storage end. Please clarify.	Wherever PIM data is stored it should be encrypted
138	**84**	ANNEXURE 9 - VOLUMETRIC/ 1. Privilege Identity Management	General Clarification 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	Could you please provide us the following information: Number of privileged IDs for check-in and check-out for Shared access Number of concurrent users expected Types of target resources and identity providers Number of applications (and types) and associated application identity for Application identity management Kindly share the inventory of the devices, applications, databases, OS, NW in scope including make, model, type, quantity and location-wise split.	Total number of privilege users is 100. Inventory of devices will be shared with the successful bidder.
139	84	ANNEXURE 9 - VOLUMETRIC/ 4. Security Information and Event Management	Security Information and Event Management • HA at DC & HA at DR • EPS - 10000 Scalable to 20000	In the volumetric details for SIEM its given 10000 EPS scalable to 20000. Could you please confirm what volume of EPS (Events Per Second) we should consider as Average EPS for sizing the SIEM solution? Please clarify whether bidder has to quote for 10000 or 20000 licenses at day one.	10,000 EPS from day 1. The solution should be upgradable to 20,000 EPS at a later stage without any changes to hardware
140	84	ANNEXURE 9 - VOLUMETRIC Database Activity Monitoring	No of Active Database instances – 7 Scalable to 20	Kindly share the inventory of databases in scope including make, model, type, quantity and location-wise split.	10 in DC and 10 in DR. If UIIC needs, the licenses should be moved between locations
141	86	DDoS	Device should be Common criteria certified at least EAL 3 or above	Should should not limit to EAL3+ but also should include other regulatory compliances.. **Recommendation**: The Regulatory Compliance should be allowed to be provided from other regulatories such as ((((UL60950-1/CSA 60950-1 (USA/Canada); EN60950-1 (Europe); IEC60950-1 (International), CB Certificate & Report including all international deviations; GS Certificate (Germany); EAC-R Approval (Russia); CE—Low Voltage Directive 73/23/EEE (Europe); BSMI CNS 13436 (Taiwan); KCC (South Korea); RoHS Directive 2002/95/EC (Europe))	As per RFP
142	89	DDoS	The ERT should support the following advanced services: 1) 24/7 monitoring of the customer's service 2) Real-time response to any threat detected 3) Direct "hot-line" access 4) Diverting the traffic when encountering a volumetric attack 5) Sending the customer a summary of each real-time attack case 6) Sending the customer a monthly report containing all threats 7) Periodically reviewing the network-security configuration	Please clarify if your looking for OEM cloud mitigation services or in country Service provider.	Cloud OEM only

143	89	ANNEXURE 10 -Technical Specifications A. PIM, point number 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.	Request to clarify the recording needs to be stored or retained for max how many days ?	180 days
144	89	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM / Point: 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.	When redundancy is built in at the collector level and log retention policy is well defined(both online and offline), 15 days of log retention at receiver is too long time, this would affect the real-time monitoring on the solution. Since we are factoring redundancy in the overall architecture, for log collectors we are considering high availability and other modules have redundancy between DC and DR. Considering redundancy at each layer 15 days of log retention is not required at log collectors. Requesting to change the clause as " 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 end in case of connection to SIEM management is lost shall be at least 2 to 3 days."	**Revised:** Retention period that must be facilitated at the collector end in case of connection to SIEM management is lost shall be at least 2 to 3 days
145	90	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS - SIEM, Point no. 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.	Kindly amend as solution should be based with a clear physical or logical separation of the collection module, logging module and correlation module. OEM should confirm all the components are sized for sustained 20,000 EPS consideration for Hardware sizing. Please clarify what does Applaince based means, Does Appliance based a purpose built hardware will all requisite OS and security application pre deployed at OEM manufacturing facility and shipped from there manufacturing location. Seek your clarification on this point.	Appliance means purpose built hardware with all requisite OS and security application pre deployed at OEM manufacturing facility and shipped from there manufacturing location. Hardware to be sized for 20000 EPS
146	90	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS	The log collection engine should have high availability without depending on third party solution. Logging and correlation modules should be proposed in standalone.	ANNEXURE 9 - VOLUMETRIC, Point 4 says SIEM as HA at both DC & DR wherein clause says Logging & Correlation in Standalone mode, kdinly confirm whether solution required in HA or Standalone mode for Logging and Correlation Layer at DC & DR. Log Collection Layer should be in High Availability mode, kindly clarify all other components from SIEM stand point - normalization, archieving, correlation and management conosle in stand alone mode.	All components needed for the Solution should be in HA.
147	90	SIEM (13)	It should be possible to store the event data in its original format in the central log storage	Central SAN environment is the expectation from UIIC, please clarify	The logs should be restored in original format in central storage
148	90	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM / Point: 9	The solution shall allow bandwidth management, rate limiting, at the log collector level.	Log collectors are capable of sending logs in both normalized as well as raw format ensuring no event drops which may happen in case of bandwidth throttling. Enforcing the bandwidth management may delay the logs which would affect the real-time monitoring and parsing of the logs in the right time. However this is OEM specific clause and we request to remove this specification.	As per RFP
149	90	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM / Point: 11	The solution should provide time based and forward feature at each log collection point	SOC is often blamed for being too reactive and scheduling of the logs may delay the logs which would affect the near real-time monitoring and parsing of the logs in the right time. The solution should provide real time log forwarding to ensure events are handled in a timely manner. Hence requesting to remove this specification.	**Revised:** The solution should provide real time monitoring and forward feature at each log collection point
150	91	Annexure 13	Integrity Pact	Bidder requests deletion of the fall clause. Please confirm.	As per RFP
151	91	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM / Point: 30	The solution should be able to integrate with external Asset Management DB to use asset values in security incident prioritizing process	Can be integrated with the Asset Management DB, but not the asset values. Requesting to change the clause as " The solution should be able to integrate with external Asset Management DB"	Expectation to have integration with Asset DB and have incident priotized
152	91	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	Please elaborate on this	Clause Stands Deleted
153	92	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM/ Point: 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.	IRDAI regulations, IT ACT reports are specific to use case requirement, it's not prebuilt in SIEM by default. Since SIEM reporting is customizable it's possible to have a customer specific reporting.	As per RFP
154	93	SIEM (57)	The Tier I and II storage should have the capability to authenticate logs on the basis of time, integrity and Origin	Need more clarity on this please.	As per RFP
155	93	SIEM (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.	Archieve in same SAN Storage or Secondary, bidder also should propose secondary storage if yes. Please clarify Kindly clarifiy the SIEM Event Byte size for storage calculation, all SIEM OEM have different metrics for storage calculation, even with 90 days online retention capacity, different OEM can have different metrics calculation. Kindly clarify storage sizing so that all the SIEM vendors quote the same capacity.	Bidder has to provide necessary tapes for the solution's proposed, with no additional cost to UIIC
156	93	SIEM (66)	It should be possible to define purging and retention rules for log storage.	Need more clarity on purging and retention here.	Ability to delete old logs based on need

157	93	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM / Point: 65	Solution should be capable to replicate logs in Synchronous / Asynchronous mode.	Need more details on the logs in Synchronous / Asynchronous mode. Please elaborate/explain in detail.	In synchronous replication, data can be written to the second site as soon as it hits cache in the primary site. Asynchronous replication adds a stage to the process, by acknowledging the host at the primary site when the data is written.
158	93	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM / Point: 72	Should be able to integrate with physical access control systems.	SIEM is meant to be a log management tool and understanding the information in the log is important and hence requesting to change the clause as "Solution should be able to parse the physical access control system logs natively or by custom parsing"	Logs from physical access controls should be integrated with SIEM
159	93	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM / Point: 73	Integrate with existing helpdesk/ incident management tools	Please provide/share the details on the existing helpdesk/ incident management tool in the environment.	UIIC does not have any ITSM tool
160	93	B. SIEM/Integration	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.	SIEM Application integration and UDS creation is an activity specially for applications as they could be custom in nature, we would request UIIC to restrict the future application integration. Kindly define the same.	As per RFP
161	93	B. SIEM/Integration	Integrate with NBA, IPS, IDS, Firewall, Proxy etc. to identify network security issues	SIEM as a solution has transformed over the years, Visibility is the key to any SIEM and it is not restricted to logs only. Visibility should be across Logs, Pactets and End Points. We should have Network layer visibility as a key aspect apart from logs for securtiy augmentation. We request that UIIC also incorprates network layer visibility as part of SIEM solution and have packet capture for both north/south and east/west traffic monitoring, Appliances with 1 Gbps throughput should be good to give this visibility acorss DC & DR. All Banks/Financial institutes are incorporating these aspects into ther RFP's. Request UIIC to recosnsider Network visibility as an important component of SIEM solution and add it into the specifications. All other layer of the SIEM like correlation, management remain the same and it give extra eyes to the solution.	**Accepted.** Bidder to provide the packet capture solution in standalone mode at DC & DR. Throughput of 1 Gbps with retention period of 7 days for raw logs and 30 day meta. Bidder should integrate the packet solution with SIEM and provide integrated view of logs and packets.
162	93	50	Senior Management should be able to view compliance to SLA for all SOC operations	Please clarify on this point as SLA monitoring is part of ITSM tool in general	Bidder to provide the necessary tools for the SLA/proposed solution.
163	94	DDoS	System should have inspection throughput of 500Mbps and scalable to 2 Gbps without additional hardware	Considering the increase in bandwdith utilization request to modify the scalibility of the appliance for next 5 years. **Recommendation**: System should have high performance architecture that ensures that attack mitigation does not affect normal traffic processing and should support DDoS Flood Attack Prevention Rate up to 15 Million PPS.	**Revised:** System should have inspection throughput of 500Mbps and scalable to 2 Gbps without additional hardware. System should have high performance architecture that ensures that attack mitigation does not affect normal traffic processing and should support DDoS Flood Attack Prevention Rate up to 15 Million PPS.
164	94	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS	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.	Kindly confirm does storage sizing to be considered for 10K Sustained EPS or 20K Sustained EPS ? Is it for 90 days online only or even 9 months offline data as well, kindly clarify.	Storage to be sized for 20000 EPS
165	94	ANNEXURE 10 -Technical Specifications, B. SIEM, Point 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.	Please provide a final storage requirement for Online, Offine and Archival requirement. Since the clause is contradicting with another clause below in the RFP under the section. **Page 26, 3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT 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**.	3 months online 9 months compressed and offline on tapes. Bidder to provide tapes with no additional cost to UIIC
166	94	SIEM (80)	The storage solution should have adequate redundancy for handling disk failures	Any preferred raid type from UIIC.	As per RFP

167	94	ANNEXURE 10 - TECHNICAL AND FUNCTIONAL SPECIFICATIONS/ B. SIEM / Point: 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.	This is OEM specific functionality of a particular OEM. While UIIC is having dedicated incident handling tool, its desirable to integrate the SIEM in to same platform rather than creating duplication. Requesting to change the clause as " The solution should integrate with the existing helpdesk/ incident management tools to 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..	Solution should have inbuilt capability and should support integration with external ticketing tool. UIIC doe not have any ITSM tool
168	94	B. SIEM/Availaibility	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.	Kindly clarifiy the SIEM architechure as this point contradicts point mentioned in SIEM/General "The log collection engine should have high availability without depending on third party solution. Logging and correlation modules should be proposed in standalone".	SIEM solution with all components in HA in DC and HA in DR
169	94	76	Connector Development tool/SDK availability for developing collection mechanism for home-grown or any other unsupported applications	Solution we are proposing is an AI and ML based solution and OEM provides complete assistance in developing the parsers. Any mistake in parser would affect solution's ability to detect the alert. We propose to either completely remove or include option of support from OEM.	As Per RFP
170	96	DDoS	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	Considering the DDOS attacks patterns (1. Attack size 2. PPS Packet per second) 5 MPPS is very less and any small attack can exceed this limit and appliance will not be able to process any further request. **Recommendation**: System should have normal traffic processing and Maximum DDoS Flood Attack Prevention Rate up to at least 5 Million PPS	As Per RFP
171	96	DDoS	Should support latency less than 70 microseconds and should be clearly documented in the data sheet	This point is specific to an OEM request you to change the point. **Recommendation**: Should support latency less than 80 microseconds	**Revised:** Should support latency less than 80 microseconds and should be clearly documented in the data sheet
172	97	35.4 DDoS	DDoS device should support for Burst Attack Mitigation and signature generation based on behaviour of Attack.	WRT to Signature generation based on behaviour of Attack this points to a specifc vendor. Also real time signunatures generation creates lots of false positives hence request you to remove this point	As per RFP
173	97	DDoS	System provides behavioural-DoS protection using signatures Generation	WRT to Signature generation based on behaviour of Attack this points to a specifc vendor. Also real time signunatures generation creates lots of false positives hence request you to remove this point WRT System provides behavioural-DoS protection using Signature generation this points to a specifc vendor. Also real time signunatures generation creates lots of false positives hence request you to remove this point	AS per RFP
174	97	Point 55 / Protection against Encrypted Attacks	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	Request the department to rephrase the clause as " 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 and should provide zero latency during peace time for SSL traffic" since the solution should mitigate the DDoS attacks only when an attack is detected and should not impact normal traffic	**Revised**: " 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 and should provide zero latency during peace time for SSL traffic" since the solution should mitigate the DDoS attacks only when an attack is detected and should not impact normal traffic
175	99	DDoS	Cloud Scrubbing should take / Accept Signalling from On-prem Device	Please clarify if your looking for OEM cloud mitigation services or in country Service provider. **Recommended :** Please consider in country Cloud mitigation as customer will have flexiblity to move to a different service provider incase of any issue / service related problems	OEM Cloud
176	99	DDoS	Cloud Scrubbing vendor should have 4 Tbps + of scrubbing capacity	Please clarify if your looking for OEM cloud mitigation services or in country Service provider. As 4TPS scrubbing is pointing to a specific vendeor and recommended to remove this point **Recommended :** Please consider in country Cloud mitigation of 80Gbps and as customer will have flexiblity to move to a different service provider incase of any issue / service related problems Request to remove the clause of 4 Tbps + of scrubbing capacity. Since customer expected attack minigation is only 500 Mbps. Also request customer for the cloud DDoS with in India inline or IRDA and Indian Data Privacy act. If customer is not mentioning the Cloud DDoS mitigation in India, OEM are likely to provide outside India, where customer traffic will be taken to outside India. Cloud DDoS Service providers can provide mitigation of attack traffic with in India and Outside India as well.	As per RFP. Cloud should be based in India
177	99	Section: WAF /Point No:2	The hardware should have minimum 6X1G interfaces	considering future scalability also in place requesting you to change this point as **"The hardware should have minimum 6X1G and in future the same interface should support 6x10G modules and shoud also have the scalability in support 2x40G modules without phyical hardware change."**	As per RFP

178	99	Section: WAF /Point No:3	The hardware should have minimum 2X10G interfaces populated with SR module	considering future scalability also in place requesting you to change this point as **"The hardware should have minimum 6X1G and in future the same interface should support 6x10G modules and shoud also have the scalability in support 2x40G modules without phyical hardware change."**	As per RFP
179	99	ANNEXURE 10 -Technical Specifications, C. DDoS, Point 63	63. Cloud Scrubbing should be from same OEM as on premise device	Request to remove this clause, since Cloud DDoS is provided by ISP not required by OEM. Since Many of the OEM are having Cloud DDoS infrastructure out side india. Which are allowing customer traffic to go outside India, if any attack orgnating from India , OEM donot have any support to protect the attack. So request to remove this clause favor only OEM.	As per RFP
180	99	ANNEXURE 10 -Technical Specifications, C. DDoS, Point 69	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)	Request to remove all the certifications. There are related to OEM specific certifications. Cloud Ddos Providers can comply to 69.2 ISO/IEC 27001:2013 (Information Security Management Systems)	As per RFP
181	100	Section: WAF /Point No:5	Solution should be virtualization ready with OEM's own hypervisorwith minimum 5 virtual WAF instances from day 1 and scalable to 10 virtual WAF instances	Requesting you to change this point as **"Solution should be virtualization ready with OEM's own hypervisor with minimum 5 virtual WAF instances with dedicate Layer 7 Throughput of 1Gbps and scalable upto 3 Gbps per Instance from day one.."**	Clause Stands Deleted
182	100	Section: WAF /Point No:17	System should support minimum of 15000 SSL CPS with 2K bit key upgradable to 18000 SSL CPS	Considering the future growth and the throughput asked requesting you to change this point as **"System should support minimum of 15000 SSL TPS with 2K bit key upgradable to 18000 SSL TPS and should support 4K bit key"**	As per RFP
183	100	Section: WAF /Point No:18	Proposed solution should support at least 8000 ECC CPS on same device	Considering current requirement and future scalability and adaption of ECC, we request you to change the point as **"Proposed solution should support at least 8000 ECC CPS and scalable upto 15000 ECC CPS on same device"**	As per RFP
184	100	Section: WAF /Point No: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.	WAF(Web application Firewall) is a technology used to protect Web applications and it is not recommended to pass other protocol traffic through these devices, hence requesting you to modify this point as **"System should perform load balancing for HTTP and HTTPS protocols."**	Clause Stands Deleted
185	100	Section: WAF /Point No: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	WAF(Web application Firewall) is a technology used to protect Web applications and it is not recommended to pass other protocol traffic through these devices, hence requesting you to modify this point as **"System should have predefined Layer 7, application level health checks (HTTP, HTTPS) and customized Layer 7 health checks for any binary and text based protocols."**	**Revised**: System should have predefined Layer 7, application level health checks (HTTP, HTTPS) and customized Layer 7 health checks for any binary and text based protocols.
186	101	Section: WAF /Point No:29	Should have Global server Load Balancing license from Day 1 without any restriction on DNS query per second	WAF(Web application Firewall) is a security technology used to protect Web applications and it is not recommended to pass other protocol traffic through these devices as this will increase the attack surface, hence **requesting you to remove this point**	Clause Stands Deleted
187	101	Section: WAF /Point No: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	This is a vendor specific point, hence **requesting you to remove this.**	Clause Stands Deleted
188	101	Section: WAF /Point No:33	Should be able to provide compliance and reporting	As Insurance industry and business demands compliance to PCI DSS and OWASP Requesting you to change this point as **"Should have inbuilt report to identify conpliance for PCI DSS and OWASP Top 10 per application and should be able to enforce the same with simple clicks from the WAF"**	As per RFP
189	101	Section: WAF /Point No:34	WAF Should support both Negative & Positive Security for zero-day protection.	Apart from positve and negative Security model there should be advanced capabilities in WAF hence requesting you to change this point as **"WAF Should support both Negative & Positive Security, Layer 7 DDoS protection, API protection, BOT protection, Credetial attack Protection, Virtual Patching support by integarting with VAPT solution without any additional licenses."**	As per RFP
190	101	Section: WAF /Point No:40	Should Provide Application Performance Monitoring. Should Provide the Server Side, Network Side and User side latency statistics	This is a vendor specific point. Application performance monitoring is a different technology and should not be mixed with an application security appliance, **hence requesting you to remove this point.**	Clause Stands Deleted
191	101	Section: WAF /Point No:41	System should be able to define the SLA of the performance for the applications.	This is a vendor specific point. Application performance monitoring is a different technology and should not be mixed with an application security appliance, **hence requesting you to remove this point.**	Clause Stands Deleted
192	102	Section: WAF /Point No:54	Should support authentication Gateway	WAF and authentication gateway are two different functionalities fulfiled by two different technologies,hence requesting you remove this point. Need more clarification on this point	As per RFP

193	108	Page 108	ANNEXURE 13 - PRE INTEGRITY PACT (FORMAT) 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.	We request the UIIC to waive this provision, since all the contracts are entered under different market conditions, hence any refund of amount due to such difference in the prices should not be considered. Please modify the clause as below: The BIDDER undertakes that it has not supplied / is not supplying identical product / systems or subsystems as a whole solution with the same scope, terms and conditions within a period of 1 year prior to the bid submission date, 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 in India and if it is found within one year after signing of the contract that the same product / systems or sub systems as a whole solution with same scope and terms and conditions was supplied by the BIDDER to any other Ministry / Department of the Government of India or a PSU in India at a lower price within a period of one year before the bid submission date, 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. Request UIIC to amend the clause with - Price fall limited to the “same” services/products not similar services/products and that the terms and conditions associated with the services/products are also the same.	As per RFP
194	113	Page 113	ANNEXURE 13 - PRE INTEGRITY PACT (FORMAT) 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.	UIIC to note that they will have access only to their books of accounts and all other bidder documents available in public domain.	As per RFP
195	115	ANNEXURE 14	ANNEXURE 14 - EXISTING SECURITY EQUIPMENT AT DC & DR		No Buyback is there. Annexure 14, is revised. Pls refer the revised Annexure 14
196	38 72 of 117; Annexure-5: Bank Guarantee Format for EMD	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. The successful bidder’s bid security will be discharged upon the bidders signing the contract and furnishing the performance bank guarantee.	There is an inconsistency as for last line of the EMD format and Clause 4.6. Please clarify. Also, request UIIC to amend this point as follows since there will many customer/third party dependencies and request to please "etc" which may effect the smooth execution of the project: 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~~.	**Revised:** EMD will be refunded to the successful bidder on submission of bank guarantee and agreement copy. The successful bidder’s bid security will be discharged upon the bidders signing the contract and furnishing the performance bank guarantee.
197	NA	Generic	list of Application which long need to be integrate please provide the details.	Application which log need to be integrated on SIEM.	Will be provided to successful bidder
198	NA	Generic	SIEM Device Integration	Please provide the device volumetric count make model which need to integrate on SIEM	Will be shared with the successful bidder
199	NA	Generic	Device Monitoring tools	Please let me if any tools already having for device availability monitoring of security component or Bidder need to propose any soluation for the same.	UIIC does not have any device monitoring tool. Bidder needs to propose the necessary tool for the same, with no additional cost to UIIC.
200	NA	NA	General Clarification	Please clarify whetehr UIIC is looking for dedicated backup solution for complete infra or not. if yes, UIIC will be providing the backup solution or bidder has to propose.	Bidder has to provide necessary tapes with no additional cost to UIIC
201	NA	General	From the RFP we get the count of Security Devices and the list of applications to be monitored in the network.	The proposed tool works on Device based pricing model. Please provide device count in number of hosts and number of servers in the environment for commercial purpose.	As per RFP
202	NA	General Query	NA	Request the department to consider the clause " The solution should be from the parent OEM and not provided by a reseller or by any third party technology OEM as a white labelled solution", as UIIC can get direct support from the OEM itself which will provide better turover time from Support team in case of any technical issues.	Bidder to provide support level where UIIC can directly open case directly

Additional queries

Sl. No.	ADDITIONAL CLAUSE	ADDITIONAL QUERY	Additional Clause Requested	REPLY
1	Suggestions to include in DAM		Solution should be deployable as agent based or in-line mode or non-inline to monitor, detect and protect databases. specify the deployment flexibility.	No Change
2	Suggestions to include in DAM		Solution should provide CPU, System utilization capping capabilities on agent- based solution.	No Change
3	Suggestions to include in DAM		Solution should be able to automatically perform the load balancing for collection and processing of the DB logs.	No Change
4	Suggestions to include in DAM		be centrally manageable from a single console including pushing agent upgrades, patch updates, configurations updates, policy updates, details on central management of all architectural components of solution from single console.	No Change
5	Suggestions to include in DAM		Should detect and alert for any abnormal database user behavior, SQL injection, unauthorized or unusual queries, access to sensitive and confidential data etc in the database. It should also detect and prevent any leakage of sensitive data.	No Change

6	Suggestions to include in DAM		Solution should store audit trail within the solution in encrypted flat files	No Change
7	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		The proposed SIEM solution should have out of the box content for ATT&CK MITRE framework. Default rules should be mapped with ATT&CK MITRE techniques.	**Accepted.** SIEM solution should have out of the box content for ATT&CK MITRE framework
8	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		SIEM should handle data burst/beyond peak EPS and should not drop logs. Peak EPS should be double the sustained EPS.	**Accepted**. SIEM should not drop the logs if goes beyond sustained EPS
9	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		The SIEM Solution must have central UI for policy configurations, Rule creation & raw log search, The system should have interface to monitor health of the various components of solution and provide details like CPU usage, interface usage, disk status etc	No Change
10	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		Sensitive Fields in the logs should de-identifed so that SOC analyst should not be able to see sentitive data. Only authorized users should be able to re-identify the senstive data.	No Change
11	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		Every log event should be given a unique event id so that event can be tracked across multiple layers of SIEM.	No Change
12	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		Proposed SIEM solution should have out of the box capability to consume threat feeds from open source community like MISP, CIRCL and Default rules should be mapped with ATTACK MITRE Techniques.	No Change
13	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		The reports should be available for the following (not limited to): a). Payment Card Industry (PCI) b). ISO (Please specify all such compliance reports and indicate the numbers against each report category.)	No Change
14	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		Proposed SIEM solution should have built-in OWASP top 10 application attack reporting capabilities.	No Change
15	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		Proposed SIEM solution should have Builtinn SOAR tool and also OOB integration with market leading SOAR tools and analytics engine for detail incident analysis.	No Change
16	3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM)		Prospose SIEM Vendor Should have UEBA, Threat Analytics capabilites and offerings for future integration.	No Change
17	Suggestions to include in PAM		Bidder recommends that UIIC gives preference to India based OEM	No Change
18	Suggestions to include in PAM		Bidder recommends that PIM solution is recognized as a leader or challenger in the 2 last reports	No Change
19	General Query : Ddos and waf		Request the department to consider the clause " The solution should be from the parent OEM and not provided by a reseller or by any third party technology OEM as a white labelled solution", as UIIC can get direct support from the OEM itself which will provide better turover time from Support team in case of any technical issues.	No Change
20	New Clause		The bidder requests for the following new clauses: a. The bidder shall be entitled to terminate the contract by providing thirty days written notice provided that the Company has failed to fulfill its obligations, including payment obligations thereof and fails to remedy the same within the thirty (30) day period. b. Each party will comply with all applicable export and import laws and associated embargo and economic sanction regulations.	No Change
21	Additional inputs	we request UIIC to include" The OEM should do design validation and give a sign off on implantation saying solution has been implemented as per the OEM best practice recommendation and should do a bi annual audit confirming solution functionality and submit the report directly to UIIC	Request to add design validation and bi annual audit of the SIEM and DAM solution from OEM and submit the report directly to the UIIC since being a product company its always better to take a second opinion from OEM in product deployment and operational functioning. We request UIIC to take at least 4 days per technology audit time as scope of bi annual audit from OEM effort.	OEM should validate the implementation as mentioned in the RFP. Annual audit should be done by OEM
22	Additional inputs	we also request the UIIC to take respective technology training directly from OEM to ensure SME does the training and UIIC can avail the training content from product makes.	SOC is a well-oiled machine between people, process and technology and hence people angle needs to be addressed from customer itself and hence the suggestion. This will help the UIIC to get to know how to handle the products once they get in to operational phase.	No Change
23	Non-Payment Remedy	Additional Clause	Bidder seeks right to suspend services in the event of delay in payment of undisputed invoice.	No Change
24	Excused Performance	Additional Clause	Any failure or delay of Bidder in performance of its obligations under this RFP/Agreement is excused to the extent such failure or delay is solely attributable to UIIC. In such event, UIIC and Bidder shall mutually agree upon extension of time and additional charges as required.	No Change
25			We request UIIC team to add this following clause "The solution should have its presence in Gartner Magic quadrants in Leaders or Challengers".	No Change
26	Additional Suggestion - DDoS	NA	Request the department to consider the clause " The proposed DDoS solution should be completely stateless to mitigate the DDoS attacks" since DDoS attacks are targeted towards Stateful devices to consume their resources and bring down the network.	No Change
27	Additional Suggestion - WAF	NA	Request the department to consider the clause " The proposed WAF solution should support VRRP protocol for automatic failover in case of device failure" since VRRP is an open standard protocol and is widely adopted in the industry by multiple network devices	No Change
28	Additional inputs		Please include the clause "The solution should be made in India"	No Change
29	Additional inputs		Please include the clause "The solution should be leading, mature and widely used brand that has been in existence for at least 5 years"	No Change

30	Additional inputs		Please include the clause "The solution should have its presence in Gartner Magic quadrants in Leaders or Challengers"	No Change
31	Suggestions to include in PAM		Bidder recommends that UIIC gives preference to India based OEM Bidder recommends that PIM solution is recognized as a leader or challenger in the 2 last reports	No Change
32	General Query : Ddos and waf		Request the department to consider the clause " The solution should be from the parent OEM and not provided by a reseller or by any third party technology OEM as a white labelled solution", as UIIC can get direct support from the OEM itself which will provide better turover time from Support team in case of any technical issues.	No Change
33	New Clause		The bidder requests for the following new clauses: a. The bidder shall be entitled to terminate the contract by providing thirty days written notice provided that the Company has failed to fulfill its obligations, including payment obligations thereof and fails to remedy the same within the thirty (30) day period. b. Each party will comply with all applicable export and import laws and associated embargo and economic sanction regulations.	No Change
34	Non-Payment Remedy	Additional Clause	Bidder seeks right to suspend services in the event of delay in payment of undisputed invoice.	No Change
35	Excused Performance	Additional Clause	Any failure or delay of Bidder in performance of its obligations under this RFP/Agreement is excused to the extent such failure or delay is solely attributable to UIIC. In such event, UIIC and Bidder shall mutually agree upon extension of time and additional charges as required.	No Change

2. ANNEXURE 7 - COMMERCIAL BID FORMAT [ALL AMOUNTS SHOULD BE IN INR] (Revised)

ANNEXURE 7 - COMMERCIAL BID FORMAT [ALL AMOUNTS SHOULD BE IN INR] (Revised)

[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											
2	SIEM											
3	DDoS											
4	WAF											
5	DAM											
6	AD – Cleanup Activity		Service	2								
8	Hardware Cost of Next Generation Firewall			2								
9	Any other item, if any											
10	Any other item, if any											
11	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	2							
4	Support Executive (L1) for DR	1							
5	Support Executive (L1) at HO for Active Directory (Mon-Fri, 9:00 - 18:00 hrs)	1							
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)		

S. No.	E. Description (Rack)	UNIT PRICE	QTY	TOTAL PRICE
1.	Rack for Data Centre		1	
2.	Rack for Disaster Recovery site		1	
TOTAL (E)				

GRAND TOTAL (A+B+C+D+E)	

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

3. ANNEXURE 14 - EXISTING SECURITY EQUIPMENT AT DC & DR (Revised)

ANNEXURE 14 - EXISTING SECURITY EQUIPMENT AT DC & DR (Revised)

Below mentioned list of devices are currently used by UIIC and is considered for reference:

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

4. REVISED TERMS & CONDITIONS (Forming Part of Original RFP)

REVISED TERMS & CONDITIONS (Forming part of Original RFP)

TECH SPEC

3.1 SCOPE OF WORK - OVERVIEW

Existing: (Pg. No. 14, 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.

Revised:

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.

All Power strips, Power cables, Network cables, Fiber cables, patch cords (copper , fiber etc.), power cords, sockets, other components needed for mounting devices in the racks and making it functional should be brought by the bidder with no additional cost to UIIC. Further, any other components required for successful implementation of the solution are to be supplied and commissioned by the successful bidder at no additional cost to the UIIC. These cables should be factory crimped cables. Also, tagging should be done at the network devices side/SOC devices/server side and wherever applicable by the bidder.

Existing: (Pg. No. 14, 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.

Revised:

a. Patches have to be applied in the production environment within 15 days of release of patches by the OEM and approved by UIIC.

b. All major updates/upgrades have to be applied in Production, within 30 days of release of updates/upgrades by the OEM and approved by UIIC.

c. 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.

TECH SPEC

3.2.1 IMPLEMENTATION & INTEGRATION

Existing: (Pg. No. 17,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.

Revised:

The bidder should note that the production (DC), DR(failover) should be physically separated. UIIC does not need non-production environment (UAT/Pre-production)

TECH SPEC

3.2.2 MEASURE & MANAGE FUNCTION

Existing: (Pg. No. 18,iii)

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

Revised:

Manage Services Resources should have at least 3 years of relevant experience in providing the Operation & Maintenance Services for Security solutions. L1 resources should have certification(s) in the field of IT security from OEMs/reputed certifying bodies.

TECH SPEC

3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT

Existing: (Pg. No. 27)

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.

Revised:

90 days of online storage, 9 months of compressed storage should be maintained by the bidder with no additional cost to UIIC (Total 1 year at any point of time i.e. 90 days online & 9 months compressed storage). Post 9 months, offline logs are to be exported to TAPE/drives. It is the responsibility of bidder to maintain offline logs beyond this 1 year period till the expiry of the contract i.e. 5 years.

The required TAPE libraries/drives need to be provided by bidder, with no additional cost to UIIC.

TIMELINES

27. PROJECT TIMELINES

Existing: (Pg. No. 14, xiii)

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.

Revised:

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	vii. PIM viii. SIEM ix. DDoS x. WAF xi. DAM xii. AD Migration	Delivery of Hardware / appliance and licenses.	8 weeks to 10 weeks from the Date of Issuance of PO
		Installation, commissioning and Implementation	28 Weeks from the Date of Issuance of PO

NOTE:

h. 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.

i. 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.

j. 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.

k. 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.

l. 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.

m. 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.

n. In the event of delayed migration / commissioning / documentation i.e after 19 (Nineteen) 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.
   iv. 1% for the first week;
   v. 2.5% for the second week; and
   vi. 5% for the third week and above.

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

ELIGIBILITY CRITERIA

3.1 ELIGIBILITY CRITERIA FOR BIDDERs/OEMs & ANNEXURE 6 - ELIGIBILITY CRITERIA FORM

Existing: (Pg. No. 10 & 75, k)

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	Purchase order copy / Project Sign off document / Client Certificate should be attached as proof.	OEM

	3. DAM 4. WAF 5. DDoS		

Revised:

k.	**For SIEM** The proposed OEM solution mentioned above 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. **OR** 2 BFSI/ PSU/ Central Govt. Defense organization in India with a minimum of 10,000 EPS (scalable to 20,000 EPS) reference customer base.	Purchase order copy / Project Sign off document / Client Certificate- mentioning one among Make, Model of Solution or EPS count implemented should be attached as proof.	OEM
	For PIM, DAM, WAF, DDoS, Next Generation Firewall Each of the proposed OEM solution mentioned above 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. **For Next Generation Firewall** Manufacturer [OEM] of the proposed Firewall solution should fall in the Gartner Magic Quadrant for Enterprise Network Firewalls as a Leader in the latest Magic Quadrant.	Purchase order copy / Project Sign off document / Client Certificate should be attached as proof. Copy of Gartner's "Magic Quadrant for Network Firewalls".	

TECH SPEC

B. SIEM

Existing: (Pg. No. 90, Sr. No. 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.

Revised:

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 end in case of connection to SIEM management is lost shall be at least 2 to 3 days.

TECH SPEC

C. DDoS

Existing: (Pg. No. 95, Sr. No. 4)

System should have inspection throughput of 500Mbps and scalable to 2 Gbps without additional hardware

Revised:

System should have inspection throughput of 500Mbps and scalable to 2 Gbps without additional hardware. System should have high performance architecture that ensures that attack mitigation does not affect normal traffic processing and should support DDoS Flood Attack Prevention Rate up to 15 Million PPS.

TECH SPEC

C. DDoS

Existing: (Pg. No. 95, Sr. No. 6)

Should support latency less than 70 microseconds and should be clearly documented in the data sheet

Revised:

Should support latency less than 80 microseconds and should be clearly documented in the data sheet

TECH SPEC

C. DDoS

Existing: (Pg. No. 98, Sr. No. 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

Revised:

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 and should provide zero latency during peace time for SSL traffic since the solution should mitigate the DDoS attacks only when an attack is detected and should not impact normal traffic.

TECH SPEC

D. WAF

Existing: (Pg. No. 101, Sr. No. 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

Revised:

System should have predefined Layer 7, application level health checks (HTTP, HTTPS) and customized Layer 7 health checks for any binary and text based protocols.

EMD

1.6 REFUND OF EMD

Existing: (Pg. No. 38)

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.

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

Revised:

EMD will be refunded to the successful bidder on submission of bank guarantee and agreement copy.

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

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

Existing: (Pg. No. 42)

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.

Revised:

13.1 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.

13.2 UIIC reserves right to shift DC/DR anywhere in India during the contract period. The bidder should dismantle, decommission, commission, install, mount, un-mount and perform reinstallation and configurations including necessary cabling and asset labelling. However, the transportation of devices to desired locations will be provided by UIIC.

5. ADDITIONAL CLAUSES TO BE CONSIDERED AS A PART OF THIS RFP

Clause : B. SIEM (Under section Integration) – Page No. 94

xx. Bidder to provide the packet capture solution in standalone mode at DC & DR. Throughput of 1 Gbps with retention period of 7 days for raw logs and 30 day meta. Bidder should integrate the packet solution with SIEM and provide integrated view of logs and packets.

Clause : 3.2.4.4 SECURITY INFORMATION & EVENT MANAGEMENT (SIEM) (Under Section SOLUTION IMPLEMENTATION) – Page. No. 26

vii. SIEM solution should have out of the box content for ATT&CK MITRE framework

viii. SIEM should not drop the logs if goes beyond sustained EPS

Clause : 3.2 DETAILED SCOPE OF WORK (Under section 3.2.1 - IMPLEMENTATION & INTEGRATION) – Page NO. 16

xxi. Bidder to provide ITSM tool with device monitoring for minimum 100 devices (network/security devices) including devices proposed in this RFP at no additional cost to UIIC.

xxii. OEM should validate the implementation as mentioned in the RFP. Annual audit should be done by OEM

xxiii. During the installation, the bidder shall check physical availability of items as per the packing list. If any of the items are not delivered / not as per the specification / are damaged etc., the bidders' representative/s at the site shall take immediate steps and ensure all the items are delivered so that the installation is not hampered. The Bidder shall have to arrange for all testing equipment and tools required for installation, maintenance, and also arrange the vehicle for transport at no additional cost to the UIIC

xxiv. In case damage of the property owned / leased by the UIIC during hardware delivery and installation which is attributable to the bidder, bidder has to replace the damaged property at his own cost.

xxv. The bidder shall ensure compatibility of the hardware, software and other equipment that they supply with the hardware and software systems being used in the UIIC.

xxvi. Implement the backup solution and tape solution adequately at DC and DR. Bidder has to factor the cost of this backup solution.

xxvii. Each of the racks existing in UIIC at DC and DR has maximum power per rack as 7.5 KVA and these racks are compatible with C13 & C14 power connectors. The proposed security devices should be compatible with C13-C14 power connectors.

xxviii. None of the proposed/supplied security equipment's should have industrial plugs & socket as connectors.

ANNEXURE 17 - UNPRICED BOM FOR SECURITY EQUIPMENT

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

S.NO.	ITEM	QTY	MAKE & MODEL
1.	SIEM		
2.	PIM		
3.	DAM		
4.	WAF		
5.	DDoS		
6.	Next Generation Firewall		
7.	Racks		

Signature :
Name :
Designation :
Date :

Company Seal

6. SUPPLY, INSTALLATION & MAINTENANCE OF FIREWALL FORMING PART OF THIS RFP

3.2.4.7 - SUPPLY, INSTALLATION & MAINTENANCE OF FIREWALL - Next Generation Firewall

SCOPE OF WORK

A. Broad Scope of work will include but not restricted to the following:

a. The Hardware appliances proposed by the bidder should have dual/ redundant power supply for each firewall/components at HO and configured on High Availability architecture.

b. The Hardware appliances proposed by the bidder should be rack mountable at HO.

c. Supply and installation of Firewall at HO as per technical specifications given in technical bid along with necessary hardware, software, licenses, accessories and necessary documentation etc.

d. 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.

e. All Power strips, Power cables, Network cables, Fiber cables, patch cords (copper , fiber etc.), power cords, sockets, other components needed for mounting devices in the racks and making it functional should be brought by the bidder with no additional cost to UIIC. Further, any other components required for successful implementation of the solution are to be supplied and commissioned by the successful bidder at no additional cost to the UIIC. These cables should be factory crimped cables. Also, tagging should be done at the network devices side/SOC devices/server side and wherever applicable by the bidder.

f. Ensure that the migration of the configuration has been completed and the applications are accessible from the intranet/internet zones.

g. Confirm to SLA parameters and the penalties as mentioned in this existing RFP.

h. Provide 24x7 OEM support for the equipment and software components supplied as part of this tender.

i. Provide updates, upgrades/new version for the software components during the warranty and maintenance period and installation of the same in co-ordination with our existing SOC service provider

j. All the equipment (hardware, software) supplied as part of solution should be IPv6 ready from day one and should support all the protocols.

k. All the equipment (hardware and software) should be from same OEM.

l. On-site, comprehensive BACK-TO-BACK Warranty from OEM for a period of 5 years from the date of commissioning.

m. The warranty also includes all software subscriptions (critical hot fixes, service packs, and all upgrades/updates) of all components supplied as part of solution.

n. The bidder to submit detailed RCA(Root Cause Analysis) for hardware & software related issues/failures. For any fault/downtime a detailed RCA signed by the concerned L2/L3 engineer should be submitted within 48 hours of fault occurrence.

o. Any coordination with the OEM for support should be carried out by the bidder engineer on need basis.

p. During the contract period the bidder should periodically check the firmware / operating system running on the Firewall and other components and upgrade the same to latest version as released by OEM within 07 days from the date of release.

q. The hardware supplied as part of this contract should not be declared End of Sale for period of 3 years from last date of submission of bids and should not be End of support for at least 3 years from thereon.

r. The company may, during the currency of the warranty, shift the equipment to other location(s) within the Country. The bidder needs to ensure that the OEMs and bidders warranty and support is valid across India. Further, bidder undertakes to continue to provide warranty and support the goods at the new location at no additional cost to UIIC.

s. Bidder will be informed about old and new location/office details as and when the company decides to shift the hardware due to operational requirements. Bidder will deploy resource(s) for decommissioning of respective equipment at old location and Commissioning of equipment at new location at no additional cost.

t. The charges towards packing, physical shifting and insurance would be borne by the company.

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

Apart from the above list, the other terms and conditions such as timelines, SLA, penalty etc. for Next Generation Firewall will be same as mentioned in this current existing RFP.

Minimum Technical Specifications

F. Next Generation Firewall – External Perimeter Gateway for HO			
Sr. No	**Functional Requirements (minimum)**	**Compliance**	**Remarks (Yes/No)**
	General Requirements		
1	Manufacturer must be referenced in the Gartner Magic Quadrant for Enterprise Network Firewalls as a Leader in the latest Magic Quadrant.		
2	All components shall be new and of current manufacture and shall not be procured via distribution channels other than those authorized or intended by the manufacturer		
	Technical Specifications		
3	**Identify applications within the HTTP/HTTPS protocol (browser based applications):** The solution must provide an application control feature that must be able to identify the application in use within the HTTP/HTTPS protocol, as well as Mobile Applications, for any TCP Port used. Once identified, applications can be allowed, blocked and limit available bandwidth.		
4	**Identify applications outside of HTTP/HTTPS traffic (desktop applications):** The solution must provide an application control feature that must be able to identify the application in use when the traffic is not sent via HTTP or HTTP Secure (HTTPS). Once identified, applications can be allowed, blocked and limit available bandwidth.		
5	**AD/LDAP integration:** The solution must provide an interface to Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) to pull user IDs and groups that can then be used in firewall rules. Must support multiple independent AD/LDAP domains.		
6	**Enforce policy on individual users and user groups:** The solution must provide a policy to allow, deny and limit available bandwidth traffic and must be enforceable on individual users or user groups.		
7	**Support for application information feed:** The solution must provide an application control function that must allow for the importation and use of information about applications. The feed should include information about how applications are used and provide recommendations to the customer regarding actions to take if the application is discovered in use. There shall be minimum 7000+ application control.		
8	There shall be Data Classification control for minimum 600+ Data Types		
9	**User-developed application signatures:** The solution must provide the necessary interface for the customer to create, edit and deploy custom application signatures.		
10	**Application whitelist/blacklist:** The solution must provide an application control function that must allow the customer to create or import whitelists and blacklists for applications and have the lists used to enforce policy on network traffic		

11	**Identify applications within SSL protocol:** The application control feature should be able to identify the application in use within SSL traffic. Once identified, applications can be allowed, blocked and limit available bandwidth. The solution must participate in the initial SSL key exchange and then decrypt session traffic to examine the contents for attacks, including both inbound and outbound inspection based on policy, without availing of off-load to alternate system.		
12	**Redundancy in physical appliances:** The solution must support redundant hot-swappable power supplies.		
13	**Out-of-band management:** The solution must support out-of-band management interfaces (either Ethernet or serial).		
14	**System availability (active/standby):** The solution must provide two Firewalls and allow failover to support 99.999% availability in active/passive or active/standby mode.		
15	**Site-to-site IPsec VPN:**The solution must act as VPN gateways for site-to site and VPNs must support remote site recognition that is based on certificates or pre-shared key.		
16	**SSLVPN:** The solution must act as VPN gateways for SSLVPN. VPNs must support 2 factor authentication and certificates.		
17	**Signature-based IPS:** The solution must have a signature-based IPS function where the signatures are created by the manufacturer and automatically applied once they are published.		
17.1	• Detection and prevention of vulnerabilities.		
17.2	• Detection and prevention of protocol misuse.		
17.3	• Detection and prevention of malware communications.		
17.4	• Detection and prevention of tunnelling attempts.		
17.5	• Detection and prevention of covert channel communications.		
18	**DoS protection:** The solution must include the mechanism to protect itself from basic Denial of Service (DoS) attacks, such as flooding and resource consumption attacks, and application layer DoS for Web applications.		
19	**User developed signatures for IPS:** The solution must provide the necessary interface for the customer to create, edit and deploy custom IPS signatures.		
20	**Administrator audit:** The solution must ensure that all administrative actions be logged to include the action taken, a time stamp, and the source IP address of the endpoint used to make the change and the administrator user ID.		
21	**SIEM integration:** The solution must be capable of sending logs to a Proposed SIEM system		
22	**Export of log information:** The solution must be capable of exporting log information in multiple formats (minimum comma-separated values (CSV) or PDF)		
23	**Role-based administration:** The solution must provide Role-based administration (RBA).		
24	**Rule usage statistics:** The solution must provide the administrator		

	with statistics on rule usage.		
25	**Traffic profile verification:** The solution must provide a search/filter mechanism to list rules matching specified criteria.		
26	**Geolocation:** The solution must provide traffic control based on country or location.		
27	**Dynamic Host Configuration Protocol (DHCP) server and relay:** The solution must provide a DHCP server and relay function.		
28	**Routing protocols:** The solution must provide at a minimum, the following routing protocols; static, OSFP and BGP		
29	**Ipv6 Support:** The solution must be Ipv6 dual stack ready.		
	Support & Maintenance		
30	Manufacturer must include 5 years of 24*7 hardware & software support, threat intelligence subscription and any other annual fee required as part of the bidder's solution.		
	Compatibility and Sizing		
31	The solution must include Four (4) 10Gbps (SFP) and Four (4) 1 GBPs (SFP) and 8x 10/100/1000Base-T RJ45 port card copper interface requirements from the Day1		
32	The solution must have min 32 Gb RAM in both primary & HA firewalls Should have minimum 240 GB of SSD on both primary & HA firewalls		
33	Firewall Security throughput shall be 12 Gbps where combined throughput for Firewall, IPS and Application Control shall be 5 Gbps and combined security throughput Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection		
34	Total Firewall Throughput shall be min 12 Gbps(12) with IPS throughput of 6 Gbps Threat Prevention 2.5 Gbps or more		
34.1	• IPS		
34.2	• application visibility		
34.3	• malware protection		
34.4	• SSL inspection		
35	Minimum 70,00,000 concurrent connections		
36	Minimum 80,000 new connections per second		
37	Minimum of 1000 Site to site IPsec VPN tunnels, 2Gbps using AES128		
38	1024 VLANs		
	Support & Licensing		
39	Enterprise Support 24X7 for 5 years from Manufacturer		
40	License For Both Primary & HA Firewall with next generation firewall including intrusion protection for min 5 year		
41	All Licensing should be per device and not user/IP based (should support unlimited users).		

42	All solutions hardware/software provided should not be having EOS/EOS/EOL announced. Proposed model should not be End of Sale within one year		
43	The Product OEM should have its own Direct Technical Assistance Centre in India.		

DELIVERY LOCATION

For the purpose of solution/equipment of Firewall implementation, the location of site is as follows:

Head Office Location:

UNITED INDIA INSURANCE COMPANY LIMITED
Head Office, NALANDA, #19, 4th Lane,
Nungambakkam High Road,
Chennai – 600034

7. SUPPLY AND INSTALLATION OF RACKS FOR SECURITY DEVICES FORMING PART OF THIS RFP

3.2.4.8 - SUPPLY AND INSTALLATION OF RACKS FOR SECURITY DEVICES FORMING PART OF THIS RFP

SCOPE OF WORK

All Power strips, Power cables, Network cables, Fiber cables, patch cords (copper , fiber etc.), power cords, sockets, patch panels, PDU, blanking panels, rails, cable management other components needed for racks and making it functional should be brought by the bidder with no additional cost to UIIC.

The bidder should mount and install the proposed security devices forming part of this RFP in these 42 U racks (1 each in DC and DR). In addition, if needed, UIIC may be providing an additional 20U rack space spread across 02 existing network racks.

Apart from the above list, the other terms and conditions such as timelines etc. for racks will be same as mentioned in this current existing RFP.

Minimum Rack Specifications

The bidder is free to propose a rack model with better specifications suiting the needs of the proposed security devices.

The intent is to propose a rack that suits the mounting/installation/functioning of the supplied security devices with no additional cost to UIIC whatsoever.

The Type and quantity of no. of socket as well as power cord along with PDU should be supplied along with the rack as suitable for the supplied security equipment's.

	G. RACK			
Sr. No	**DC & DR RACK SPECIFICATIONS**		**Compliance**	**Remarks (Yes/No)**
1.	Network Rack Specifications	• 800 x 1000mm 42 RU rack		
		• Two PDUs for each rack		
		• Locknuts to rack mount devices		
2.	PDU Specifications	• IEC PDU with 24 sockets		
		• C13-C14 power chords for all the sockets		
3.	DC Rack	• Double door rack for both Front & Back		
4.	DR Rack	• Single door rack for both Front & Back		

DELIVERY LOCATION

For the purpose of solution/equipment of racks, the location of site 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..