Request for Proposal for procurement of User and Entity Behavior Analysis Solution - NPCI/RFP/2019-20/IT/26 dated 24.12.2019			
Description in RFP	**Clarification Sought**	**Additional Remarks (if any)**	**NPCI Response**
The Equipment's quoted/supplied by bidder should not be declared as EOL or EOS by the OEM Within/from three (3) years of releasing PO	Hope "EOL or EOS" means end of life or end of support only. Request clarification on this.		EOL is "End of Life" and EOS is "End of Support"
Bidder should provide design, size, supply, implement and maintain the solution, Security Policy Change Automation including hardware, Software, OS license (core based), database license (core based with unlimited device/ user access etc. for the period of contract.	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infrastructure devices for scope across the project period.
Bidder to factor and propose both hardware based solution and software based solution as per their architecture which includes associated monitoring and management software(s) including OS license (core based), database license (core based with unlimited device/ user access etc. any.	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infrastructure devices for scope across the project period.
Execute User Acceptance Test (UAT) for the UEBA solution, i.e. execute known bad hacking attempts and suspicious activities	Please confirm if UAT testing can be done on the production setup or we need to factor separate UAT server		Separate UAT Setup needs to be factored
Bidder should work with the existing System Integrator(s) of the NPCI to integrate the solution with Active Directory, SIEM Solution, server and storage environment, enterprise network, EMS / NMS solution, security solution, ticketing tools etc.	Request you to share the details for all the said solutions.		Details will be provided to Technically qualified bidder
The bidder should have reported minimum annual turnover of Rs. 13 Crores as per audited financial statements in each of the last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019) and should have reported 5% profits (profit after tax) as per audited financial statements in at least two of last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019).	Request NPCI to consider the clause as "The bidder should have reported minimum annual turnover of Rs. 13 Crores as per audited financial statements in each of the last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019) and **should have reported profits (profit after tax) as per audited financial statements in at least two of last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019).** **Or** The bidder should have reported minimum annual turnover of Rs. 13 Crores as per audited financial statements in each of the last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019) **and should have reported 3% profits (profit after tax) as per audited financial statements in at least two of last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019)."**		Refer Corrigendum 1
Period of operations in required domain: Minimum 3 years preceding the bid participation or 3 successful customer implementation into production and handling transaction	Hope the bidder should have experience in Cyber Security Domain. Please confirm.		Yes, your understanding is correct
Partner/SI should not be associated with NPCI in any assignment related to Device Audit/Security Audit/Monitoring of device/Security monitoring.	Request NPCI to remove this clause		No change in RFP
If revised BOM is not shared within 3 days post technical presentation (with commercials to IT procurement and BOM without commercials to business user team)	3 days is too little a time to rework the BOM and commercials	Kindly help with atleast 10 working days.	No change in the RFP
Supply, installation, maintenance and post implementation support for the entire User and Entity Behavior Analysis (UEBA) Solution (Hardware, Software, License for OS core based, license for DB core based with unlimited device/user integration). Bidders to provide the item wise details along with quantity in Bill of materials	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infrastructure devices for scope across the project period.
(iii) Liquidated damages will continue to be levied for delays in delivery as per the terms of the PO, if the delays are attributable to the vendors.	Request NPCI to confirm the maxmum CAP of Liquidated damages.		No change in RFP
Delivery of hardware, software, and license should be within 6 weeks.	Request you to change this to "Delivery of hardware, software, and license should be within 8 weeks."		No change in the RFP
Installation & commissioning should be completed in next 10 weeks.	Request you to change this to "Installation & commissioning should be completed in next 14 weeks."		No change in the RFP
NPCI reserves the right to place Purchase Orders with the selected bidder(s) for any or all of the goods and/or services at the agreed unit rate for individual categories of purchase order during the period of 1 year from the date of award / 1st Purchase Order.	Request NPCI to Limit the price validity for the repeat order to a maximum period of 180 days from the price discovery date.		No change in RFP
The solution should have permission for device admin, subnet admin, audit log, edit model and advanced search, etc.	Need more details over this point especially Subnet Admin		Proposed solution should mention on how role based access is done in the solution.
Execute User Acceptance Test (UAT) for the UEBA solution, i.e. execute known bad hacking attempts and suspicious activities	Is NPCI looking for us to propose compute required for UAT? and also is NPCI looking to setup UAT for UEBA.		Separate UAT Setup needs to be factored

Solution should support installation on Windows and Linux environment	Most of the solutions support installation on Linux platform. We request to change it to below: Solution should support installation on Windows or Linux environment		Bidder to eloborate the platform on which the solution works
Solution installation should support Docker Containers & Virtual cloud for easy, deployment and building on premises	As most of the solutions are still upgrading solution to be deployed on docker containers; we request to change it to below: Solution installation should support Docker Containers or Virtual cloud for easy, deployment and building on premises		We expect the solution to support various virtualized paltforms. This clause can also be read as virtual cloud/docker containers.
Customer BFSI reference in India Please provide at least 2 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been using your product? e. Contact name, title, email and direct telephone number f. Which solution deployed.	Being a security product; most of the BFSI enterprises don't agree to give direct reference and as part of NDA most of the OEM's cannot give reference. Hence we request this clause to change it to below: Customer BFSI/Non-BFSI reference in India/World Wide Please provide at least 2 India/World Wide References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been using your product? e. Contact name, title, email and direct telephone number f. Which solution deployed. or OEM can provide confirmation of having reference on thier letter head if in case of OEM has NDA with customers.		No change in RFP
UEBA should be intelligent and should automatically tweak itself through automated learning, and also support creation of custom models	Most of the leading UEBA solutions are intelligent and should tweak itself through automated learning and also models are built by data scientist who understands data and usecase then builds the models. We request NPCI to change it to below: UEBA should be intelligent and should automatically tweak itself through automated learning, and also support creation of custom models or should have it in roadmap to support the same.		Custom model creation should be available in the solution. If creation of custom models is not available currently then it should be available in roadmap of the solution proposed.
The solution should have permission for device admin, subnet admin, audit log, edit model and advanced search, etc.	UEBA solution role based access should be based on tenants. This helps to seggregate users based on the group of users and then give access to specific tenants. We request to change it to below: The solution should have permission for device admin, subnet admin, audit log, edit model(or edit model should be in roadmap) and advanced search, etc. or should support multi-tenancy which should segregate data and access by tenant.		Proposed solution should mention on how role based access is done in the solution.
The solution should allow administrators to modify model formula	Model formula are very critical for any UEBA solution and should not be changed as this will induce lot false positives. As you have already asked for custom models; Hence we request this to change it to below: The solution should allow administrators to disable any model formula and build custom models or custom model building should be available in future roadmap.		The solution should allow to disable models if required. We understand that modifying model formula is like creation on of custom models. This should be read as creation of custom models may be from existing models.
Should be able to show us RAW packet headers, or relevant data basis on which anomalous behaviour was observed	As Most of the UEBA solutoins work on logs and detect threats accurately. This also looks specific to one particual OEM. We request to please remove PCAP's and change it to below: Should be able to show us RAW logs, or relevant data basis on which anomalous behaviour was observed		The specification already has RAW packets or relevant data. Please provide details of what relevant data solution can show on which anamalous behaviour was observed.
The solution should allow administrators to define new models/new rules for threat scenario specific to organization	Defining New Models should be done by highly skilled technical personal and not just by administrator; as he has to understand algorithm, data and the output of the algorithm. A Data Scientist is the best fit for this activity. Hence we request to change it to administrator/data scientist. Hence we request to change this spec to below: The solution should allow administrators/Data Scientist to define new models/new rules for threat scenario specific to organization.		No change in the RFP
Should allow administrators to upload PCAPs for analysis	As Most of the UEBA solutoins work on logs and detect threats accurately. This also looks specific to one particular OEM. We request to change it to below: Should allow administrators to upload Logs for analysis		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory

Use of unsupervised and supervised machine learning algorithms	Every UEBA solution works differently. Some UEBA solutions detect threats with the help of supervised learning, some with unsupervised and some with both. Supervised learning is one subset of Machine Learning with the help of lables. Unsupervised machine learning finds new patterns in large sets of data, no matter how random that data seems. The algorithms collect data and cluster it to find structures and recognize emerging patterns. This type of machine learning is particularly well-suited to insider threat detection because inside(r) threat scenarios typically deal with limited, labelless datasets. We request to change to below: Use of unsupervised/supervised machine learning algorithms.		The bidder to mention clearly on weather supervised machine learning or unsupervised machine learning is used. Also the revised specification is as below: Use of unsupervised/supervised machine learning algorithms.
Ability to define custom peer groups and perform behaviour analysis	Peer grouping is done differently in each UEBA solution. The ability to dynamically, mathematically identify unique baselines for peer groups reduces false positives. Hence we request to please make it custom/automatic peer grouping Ability to define custom peer groups/dynamic peer grouping through mathematically identifying unique patterns and perform behaviour analysis		No change in the RFP
Ability to build custom behaviour models without requiring any development effort	We request you to change it to below: Ability to build custom behaviour models without requiring any development effort or this feature should be in roadmap		Custom model creation should be available in the solution. If creation of custom models is not available currently then it should be available in near future roadmap of the solution proposed.
Proposed solution should mention on how role based access is done in the solution.	UEBA solution role based access should be based on tenants. This helps to seggregate users based on the group of users and then give access to specific tenants. We request to change it to below: Customizable Dashboards for different tenants		Proposed solution should mention on how role based access is done in the solution.
The solution has self-learning algorithms (supervised and unsupervised machine learning) to identify patterns of normal and malicious user and entity behaviour with advanced mathematics, without any connection to cloud or third party platform	Every UEBA solution works differently. Some UEBA solutions detect threats with the help of supervised learning, some with unsupervised and some with both. Supervised learning is one subset of Machin Learning with the help of lables and Unsupervised machine learning is superior as it finds new patterns in large sets of data, no matter how random that data seems. The algorithms collect data and cluster it to find structures and recognize emerging patterns. This type of machine learning is particularly well-suited to insider threat detection because inside(r) threat scenarios typically deal with limited, labelless datasets. We therefore request to change to unsupervised/supervised machine learning. The solution has self-learning algorithms (supervised / unsupervised machine learning) to identify patterns of normal and malicious user and entity behaviour with advanced mathematics, without any connection to cloud or third party platform		No change in the RFP
The solution is a network-centric approach and allow network data ingestion including Layer 2 SPAN, Layer 3 SPAN and Network taps	Most of the leading UEBA solutions work on logs. Logs gives more accurate results and most of the AI/ML algorithms work on structered data which gives accurate results. We request to make it logs rather than packet capture or remove this clause. We request you to change it to below: The solution should be log or network-centric approach and allow network data ingestion including Layer 2 SPAN, Layer 3 SPAN and Network taps or logs should be collected from all leading security log sources.		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.
All relevant data including machine learning and alerts, flow data (history of connections), Advanced Search data, and PCAPs (Packet Capture) should be stored in the appliance.	As most of the UEBA solutions are software based solutions and works on logs. We request you to please change it to below All relevant data including machine learning and alerts, flow data (history of connections), Advanced Search data, should be stored in the appliance/server/UEBA application		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.
Exporting (PCAPs) and report generation capabilities (Excel, PDF, XML)	Most of the leading UEBA solutions have no dependency on packets and work purely on logs. We request to remove PCAPS. This is also specific to one particular OEM.		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.
Sensitive data leakage: User manipulates http request / response parameter to download sensitive data	Which solution will detect the changes of HTTP Request? UEBA will detect the user behavior? How is NPCI going to share these logs with UEBA to detect? Please help to clarify this usecase.		Bidder to mention how data exfilteration attempts are identified by proposed solution.

The solution's UI should be able to play-back particular events in a graphical way	Play back of events is primarily a functionality of packet capture. Sequence of events needs to be shown in graphical way so that analyst can analyze events and the sequence of activity performed by the user. Hence we request to change it to below: The solution's UI should be able to play-back or show sequent of events or activities performed by user in a graphical way		The solution's UI should be able to play-back or show sequence of events or activities performed by user/entity in a graphical way for a specific period of time, example 7 days, 15 days, one month and 3 months
Allows us to create Incidents out of Events/alerts onto which analysts will collaborate inputs and for which, reports can be exported	This is a functionlity of a SOAR platform or SIEM platform. UEBA is not a incident management platform. Hence we request to remove this clause or change it to below: Proposed UEBA solution should be integrable with all leading SIEM and SOAR Platforms		This specification should be read as proposed solution should be able to integrate directly with all SOAR platforms and SIEM's for this functionality.
Bidder should provide design, size, supply, implement and maintain the solution, Security Policy Change Automation including hardware, Software, OS license (core based), database license (core based with unlimited device/ user access etc. for the period of contract.	Kindly elobrate on what is the exact requirement of "Security Policy Change Automation"		Security policy change means; defining new models for new threats as per new threat landscape or compliance requirements.
To configure UEBA solution at Primary DC and Disaster Recovery site having high availability	Do we have to implemet the solution in HA in DC and HA in DR respectively ?		Yes
Bidder should provide support for O/S and D/B hardening (per the policies defined by NPCI) for the servers that will be provided by bidders.	Is NPCI looking for onsite support from bidder on 24x7 basis ?		hardening is done on periodic basis and expert is required to support during the scheduled activity
The selected Bidder shall appoint a single point of contact, with whom NPCI will deal with, for any activity pertaining to the requirements of this RFP.	Is NPCI looking for onsite POC from bidder ?		Person should be reachable (24 x 7) , on phone , email and webex , if the issue does not get resolved, then the person is required to be on-prem
Period of operations in required domain: Minimum 3 years preceding the bid participation or 3 successful customer implementation into production and handling transaction	Since UEBA is a very niche technology we request you to change the clause to "Period of operations in required domain: Minimum **1 years** preceding the bid participation or **1 successful** customer implementation into production and handling transaction		No change in the RFP. Bidders need to provide a self declaration stating that they have minimum years of experience in the **Information / Cyber Security domain OR** 3 sucessful implementation.
Delivery of hardware, software, and license should be within 6 weeks.	We request to change the clause to "Delivery of hardware, software, and license should be within 8 weeks"		No change in the RFP
	Kindly clarify the UEBA license required for how many users or EPS ?		EPS count is 40K
Bidder should provide design, size, supply, implement and maintain the solution, Security Policy Change Automation including hardware, Software, OS license (core based), database license (core based with unlimited device/ user access etc. for the period of contract.	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infrastructure devices for scope across the project period.
Supply, installation, maintenance and post implementation support for the entire User and Entity Behavior Analysis (UEBA) Solution (Hardware, Software, License for OS core based, license for DB core based with unlimited device/user integration). Bidders to provide the item wise details along with quantity in Bill of materials	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infrastructure devices for scope across the project period.
The solution should have permission for device admin, subnet admin, audit log, edit model and advanced search, etc.	Need more details over this point especially Subnet Admin		Proposed solution should mention on how role based access is done in the solution.
The solution should allow administrators to manage subnet by different admin accounts	Need more details over this point		Proposed solution should mention on how role based access is done in the solution.
Session Tracking of user in case of IP switch	Does this imply DHCP scenario or IP address change on single machine or a shared amchine scenario, etc. Need clarification		All the possible scenarios.
The solution is a network-centric approach and allow network data ingestion including Layer 2 SPAN, Layer 3 SPAN and Network taps	Layer-2/3 SPAN and TAPS will be equivalent to Packet Captures and will take high Storage and need parsing & normalization to facilitate analytics. Consider NETFLOW as an option from Network devices as an alternate option		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.

All relevant data including machine learning and alerts, flow data (history of connections), Advanced Search data, and PCAPs (Packet Capture) should be stored in the appliance.	PCAPs are raw data packet captures which will further take up high storage and also need parsing & normalization to facilitate Analytics. PCAPs are more relevant for Forensics solution. Kindly consider changing this clause accordingly or removing PCAPs. Alternately Meta Data or Logs from PCAPs tool can be sent to UEBA. Need your concurrence		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.
Multiple UI elements can be dragged into an incident, from metric graphs to device log entries.	Multiple UI elements or Artifacts can be dragged or uploaded into an incident, from metric graphs to device log entries.		no clarifications sought
Bidder should provide design, size, supply, implement and maintain the solution, Security Policy Change Automation including hardware, Software, OS license (core based), database license (core based with unlimited device/ user access etc. for the period of contract.	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infrastructure devices for scope across the project period.
Bidder to factor and propose both hardware based solution and software based solution as per their architecture which includes associated monitoring and management software(s) including OS license (core based), database license (core based with unlimited device/ user access etc. any.	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infrastructure devices for scope across the project period.
Supply, installation, maintenance and post implementation support for the entire User and Entity Behavior Analysis (UEBA) Solution (Hardware, Software, License for OS core based, license for DB core based with unlimited device/user integration). Bidders to provide the item wise details along with quantity in Bill of materials	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infrastructure devices for scope across the project period.
The solution should have permission for device admin, subnet admin, audit log, edit model and advanced search, etc.	Need more details over this point especially Subnet Admin		Proposed solution should mention on how role based access is done in the solution.
The solution should allow administrators to manage subnet by different admin accounts	Need more details over this point		Proposed solution should mention on how role based access is done in the solution.
Session Tracking of user in case of IP switch	Does this imply DHCP scenario or IP address change on single machine or a shared amchine scenario, etc. Need clarification		All the possible scenarios.
Should allow administrators to upload PCAPs for analysis	PCAPs are raw data packet captures which will further take up high storage and also need parsing & normalization to facilitate Analytics. PCAPs are more relevant for Forensics solution. Kindly consider changing this clause accordingly or removing PCAPs. Alternately Meta Data or Logs from PCAPs tool can be sent to UEBA. Need your concurrence		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.
The solution is a network-centric approach and allow network data ingestion including Layer 2 SPAN, Layer 3 SPAN and Network taps	Layer-2/3 SPAN and TAPS will be equivalent to Packet Captures and will take high Storage and need parsing & normalization to facilitate analytics. Consider NETFLOW as an option from Network devices as an alternate option		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.
All relevant data including machine learning and alerts, flow data (history of connections), Advanced Search data, and PCAPs (Packet Capture) should be stored in the appliance.	PCAPs are raw data packet captures which will further take up high storage and also need parsing & normalization to facilitate Analytics. PCAPs are more relevant for Forensics solution. Kindly consider changing this clause accordingly or removing PCAPs. Alternately Meta Data or Logs from PCAPs tool can be sent to UEBA. Need your concurrence		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.
Exporting (PCAPs) and report generation capabilities (Excel, PDF, XML)	Requesting for exclusion of Exporting PCAPs as PCAP may require high storage and also need further processing of data to facilitate Analytics		The bidder to mention clearly on how proposed solution functions without packet capture. Packet capture is not mandatory.
Multiple UI elements can be dragged into an incident, from metric graphs to device log entries.	Multiple UI elements or Artifacts can be dragged or uploaded into an incident, from metric graphs to device log entries.		" Multiple UI elements or Artifacts to be dragged or uploaded into an incident, from metric graphs to device log entries."
If revised BOM is not shared within 3 days post technical presentation (with commercials to IT procurement and BOM without commercials to business user team)	3 days is too little a time to rework the BOM and commercials	Kindly help with atleast 10 working days.	No change in the RFP

The bidder should have reported minimum annual turnover of Rs. 13 Crores as per audited financial statements in each of the last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019) and should have reported 5% profits (profit after tax) as per audited financial statements in at least two of last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019). In case audited financial statements for 2018-2019 are not ready, then management certified financial statement shall be considered for 2018-2019; however, this exception is not available in case of previous financial years. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this	**Request you to give relaxation on 5% PAT** and pls amend the caluse as " The bidder should have reported minimum annual turnover of Rs. 13 Crores as per audited financial statements in each of the last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019) and should have reported profit after tax as per audited financial statements in at least two of last three financial years (i.e. 2016-2017, 2017-2018 and 2018-2019).	Our turn over is more than 1000Cr and 5% PAT is not possible to get being SI	Refer Corrigendum 1
Period of operations in required domain: Minimum 3 years preceding the bid participation or 3 successful customer implementation into production and handling transaction	Request you to please relax this point for bidder as this is very niche technology and not possible for bidder to provide 3 PO refernce, Pls help to change to OEM refernces.		No change in the RFP. Bidders need to provide a self declaration stating that they have minimum years of experience in the **Information / Cyber Security domain OR** 3 sucessful implementation.
Bidder should provide design, size, supply, implement and maintain the solution, Security Policy Change Automation including hardware, Software, OS license (core based), database license (core based with unlimited device/ user access etc. for the period of contract.	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infratsructure devices for scope across the project period.
Bidder to factor and propose both hardware based solution and software based solution as per their architecture which includes associated monitoring and management software(s) including OS license (core based), database license (core based with unlimited device/ user access etc. any.	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infratsructure devices for scope across the project period.
Supply, installation, maintenance and post implementation support for the entire User and Entity Behavior Analysis (UEBA) Solution (Hardware, Software, License for OS core based, license for DB core based with unlimited device/user integration). Bidders to provide the item wise details along with quantity in Bill of materials	Consider some upper CAP on User and Device count for optimized solutioning	Kindly factor some growth factor for User and Entities for the contract period and consider that number as upper limit for solution design	Consider the user scope of 1500 Users and 2500 number of Infratsructure devices for scope across the project period.
The solution should have permission for device admin, subnet admin, audit log, edit model and advanced search, etc.	Need more details over this point especially Subnet Admin		Proposed solution should mention on how role based access is done in the solution.
If revised BOM is not shared within 3 days post technical presentation (with commercials to IT procurement and BOM without commercials to business user team)	3 days is too little a time to rework the BOM and commercials	Kindly help with atleast 10 working days.	No change in RFP