NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
1	28 GT&C - Liquidated Damages	Penalty Clause Non-compliance of the SLA as per the Table No-1, Sl.No.1, penalty would be Rs. 10,000/- per device per day for each day or part thereof, for device not functioning as per specifications (all days of the week). The overall penalty cap would be 15% of the respective component cost of the Next Generation Threat Prevention Solution. After the cap is reached, NIC may cancel the contract.	We request that overall penalty cap shall be 5% of the respective component cost of the Next Generation Threat Prevention Solution	As per RFP
2	28 GT&C - Liquidated Damages	If the Supplier fails to Deliver within scheduled period, 'NIC' shall deduct from the contract price, as liquidated damages, a sum equivalent to 0.50% of the price of the delayed goods for each week (7 days) or part thereof of delay until actual delivery, up to a maximum deduction of 10% of the value of the delayed goods. Once such delay crosses the maximum limit, 'NIC' may consider contract either full and/or, in part, and annulment of order, either full and/or, in part. C If the Supplier fails to Install, Integrate and Commission the devices (the device running live and with full functionality as per Technical Specifications in production environment) within 6 weeks from date of Delivery, 'NIC' shall deduct from the contract price, as liquidated damages, a sum equivalent to 0.50% of the price of the goods to be installed, for each week (7 days) or part thereof of delay until actual installation, integration and commissioning, up to a maximum deduction of 10% of the value of the delayed goods. Once such delay crosses the maximum limit, 'NIC' may consider termination of the contract either full and/or, in part, and annulment of order, either full and/or, in part.	We request that maximum deduction on account of late delivery or installation shall be capped at 5% of the value of the delayed goods as equipments are priced with 3 year warranty	As per RFP
3	68.2 Annexure 10 (Vol-II) – Commercial Bid	Commercial Bid-Grand Total Price (without Tax) -	Please clarify ,Grand total is with tax or without tax as below instruction shows "*The price quoted by the bidder shall be inclusive of all taxes, levies, duties and cess like GST, CGST, IGST etc, which will be paid as per the rate prescribed by Government time to time* ."	As per RFP
4	68.2 Annexure 10 (Vol-II) – Commercial Bid	The price quoted by the bidder shall be inclusive of all taxes, levies, duties and cess like GST, CGST, IGST etc, which will be paid as per the rate prescribed by Government time to time.	We request to add this clause " Any new tax introuced by government shall be in NIC's account"	As per RFP
5		This free of charge warranty shall start and shall remain valid for 3 Years for Components of Next Generation Threat Protection Solution for items supplied against RFP No. NIC/IT/RFP/NXGThreatProtect/RFP/07/2017 from the last date of installation of the equipments that has been delivered and installed, commissioned, tested and accepted.	We request that warranty should start from Delivery ,as OEM warranty starts from delivery.	Date of Implementation and completion sign-off of the individual components of the solution
6	13 GT&C - Payment will be made in the following Manner	13 GT&C - Payment will be made in the following Manner 70% Cost of all Hardware / Software / Licenses / all other accessories. Remaining Cost of respective Hardware / Software / Licenses / all other accessories related to Installation, Integration and Commissioning. Quarterly in arrears	We request Payment will be made in the following Manner:- on Delivery site wise: 80%of the Cost quoted for 5 year of all Hardware / Software / Licenses / all other accessories Remaining Cost of respective Hardware / Software / Licenses / all other accessories on Installation, Integration and Commissioning. SOC Engineer: Quarterly in Advance	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
7		Repeat order of any of the components of the Solution in respect of RFP/07/2017, may be placed with the Supplier within a period of 24 Months from the time of placement of the first Order. Any repeat purchase order from NIC to Supplier for procurement of additional components of the solution, after passage of one year from initial purchase order would be subject to the Exchange Rate Variation Clause. Also refer Section - 3 J. Exchange Rate Variation Clause Purchase of any additional component/item after one year from placement of first Purchase Order, would be linked to the ERV Clause. The conversion rate of US Dollar to Indian Rupees as on close of date of bid submission would be considered as the base rate. Any fluctuation (+ or -) 2% in the conversion rate as on the date of placement of additional purchase order, will be taken into account and benefit thereof will be passed on to either Supplier or NIC. Any effect of such fluctuation, on Taxes will also be considered.	Please take 1 year INR Price validity from OEM. After 1 year please put the same ERV clause on OEM also	As per RFP
8	41 – Indemnity	**We request that the clarity be provided in the RFP** that Indemnity shall only be restricted to third party claim for (i) IPR Infringement indemnity, and (ii) bodily injury and death and tangible property damage due to gross negligence and willful misconduct. The process of indemnification shall provide the requirement of notice, right to defend and settle, and the concept of apportionment (liable only to the extent of its claim), mitigation and carve-outs.		As per RFP
9	37 - Limitation of Liability	We request NIC to limit the Liability of the Bidder by reflecting the below mentioned clause as a corrigendum to the RFP: The Bidder’s aggregate liability in connection with obligations undertaken under the purchase order, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the Annual Contract Value. Neither party shall not be liable for any indirect, special, punitive, exemplary, speculative or consequential loss or damage.		As per RFP
10	Not there in the RFP Form of Agreement	NIC and the Bidder agree that – if the Bidder is successful and selected under this RFP then the Parties shall sign a mutually agreed Agreement.		As per RFP
11	62.Eligible Bidders	The Bidder should have implemented and maintained captive SOC for any two PSU/BFSI/Government customers (with at least 1000 locations) in India within last 3 years. SOC solution should have at least 4 out of the following components like SIEM, WAF, DAM, PIM, NBA, Anti-APT solutions/Anti-Phishing/DLP. Completion Certificates to be provided from Customer	Request to change it within last 5 years	Clause modified as "The Bidder should have implemented and maintained captive SOC for any two PSU/BFSI/Government customers in India, (with one such customer having at least 1000 locations), within last 5 years. SOC solution should have at least 4 out of the following components like SIEM, WAF, DAM, PIM, NBA, Anti-APT solutions/Anti-Phishing/DLP in atleast one reference. Completion Certificates to be provided from Customer"
12	8 GT&C – Delivery Schedule: / 28 GT&C - Liquidated Damages:	Installation, Integration and Commissioning of Next Generation Threat Protection Solution and NIC Sign-Off -- All Components of the solution in within 16 (Sixteen) Weeks Date of Delivery of equipments. If the Supplier fails to Install, Integrate and Commission the devices (the device running live and with full functionality as per Technical Specifications in production environment) within 6 weeks from date of Delivery	The Installation, Integration and Commissioning sign-off date is contradicting in both the clauses. Kindly confirm the same.	Rectified in Clause - 28 C. Sixteen Weeks from Date of Delivery

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
13	3 GT&C - Price Schedule:	The bidder in respect of RFP/07/2017 is also required to quote Commercials for Manpower (SOC Engineer) on own direct payroll to be resident at NIC HO Premises for the entire period of Contract, for the purpose of managing the requirements as under Scope of Work in respect of Next Generation Threat Protection Solution, in the	What would be the ooficial timing for the resident engineers?	8 am to 8 pm from Mon-Sat. Other days/hours in case of emergency given nature of Security Operation
14	4 GT&C – Bidder to Note:	The Bidder/Supplier would maintain appropriate and adequate stand-by equipment and spares for maintenance during the entire On-Site Comprehensive Warranty, AMC period in respect of the RFP.	Does any on-site spare to be maintained mandatorily?	As per RFP
15	Page 42 , Point 1.9	Solution should have ability to detect advanced persistent threats across all traffic including encrypted on perimeter, inspect and analyze all protocol, analyze all the files (pdf, doc, xls, xlsx, jpg, jpeg etc.) for embedded code and binary codes.	As per the scope of the RFP, we understand that NIC is looking for APT solution for Web, Email and Endpoint. Hence we would request you to please change the specs to "Solution should have ability to detect advanced persistent threats across all traffic including encrypted on perimeter, inspect and analyze all protocol (related to web and email), analyze all the files (pdf, doc, xls, xlsx, jpg, jpeg etc.) for embedded code and binary codes."	Solution should have ability to detect advanced persistent threats across all traffic including encrypted on perimeter, inspect and analyze all protocol (related to web and email and other network traffic), analyze all the files (pdf, doc, docx, xls, xlsx, ppt, pptx, jpg, jpeg, compressed files etc.) for embedded code and binary codes."
16	Page 43, Point 1.19	The proposed network advanced persistent threat component should have the ability to be deployed in the following modes: Out of -band mode inline monitoring mode Inline active blocking mode	As per the scope of the RFP, we understand that NIC is looking for APT solution in integration with existing endpoint and network security solutions. Please confirm that this deployment modes can be achieved with integration with existing endpoint and network security solutions	Bidder can propose either by integrating with the existing solution or, propose a new which should be deployable in all of the modes
17	Page 43, Point 1.22	The solution should provide detection, analysis & remidation capability against advanced persistent threat-based attacks on network, mail and endpoint systems. Real time and Offline threats should be detectable and preventable	Please provide details on expectations from offline threats	Malware get executed over period of time, therefore time based/checking of external NTP/CnC server for execution should be detected and Blocked/Quarantined/Killed
18	Page 43, Point 1.25	The Proposed solution should support atleast 500 Mbps of real world throughput on day 1 and should have the option to scale it to 1gbps / The proposed solution should be sized to scan files sent by our existing endpoint and network devices with 20% scalability	As per the scope of the RFP, we understand that NIC is looking for APT solution in integration with existing endpoint and network security solutions. Please confirm that this deployment modes can be achieved with integration with existing endpoint and network security solutions.	As mentioned in the RFP bidder can propose solution integrating with the existing solution or standalone. If standalone solution is proposed then it should meet the minimum specification as mentioned in the RFP
19	Page 44, Point 1.31	The solution should stop web-based attacks and have capability to prevent outbound multi-protocol call-backs of the malware with minimum 4 X 1GE inbuilt/populated ports	As per the scope of the RFP, we understand that NIC is looking for APT solution in integration with existing endpoint and network security solutions. Please confirm that this deployment modes can be achieved with integration with existing endpoint and network security solutions.	As mentioned in the RFP bidder can propose solution integrating with the existing solution or standalone. If standalone solution is proposed then it should meet the minimum specification as mentioned in the RFP
20	Page 44, Point 1.33	Solution must have the capability to analyze large files	Kindly mention the size of file to be analyzed	Minimum of 10 Mb
21	Page 44, Point 1.37	The proposed solution should support Multiple protocols for inspection, including but not limited to :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS, P2P etc protocols ;Internal direction :SMB etc ,Database protocol (MySQL, MSSQL, Oracle etc)	As per the scope of the RFP, we understand that NIC is looking for APT solution for Web, Email and Endpoint. This would not include databases. Hence we would request you to please change the specs to "The proposed solution should support Multiple protocols for inspection, including but not limited to :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS, P2P etc protocols ;Internal direction :SMB etc."	RFP Clause modified as follows, " The proposed solution should support Multiple protocols for inspection, including but not limited to :- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS, P2P etc protocols ;Internal direction :SMB etc"

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
22	Page 45, Point 1.49	The Solution must support for extraction of password in email body or subject-line to be used to open password protected attachments for mail sandboxing	Different OEMs have different way to accepting password protected file submissions to sandboxing solution. Hence we would request you to change the specs to "The Solution must support for extraction of password in email body or subject-line to be used to open password protected attachments for mail sandboxing or should be able to configure password for manually uploaded files."	RFP Clause modified as follows, "The Solution must support for extraction of password in email body or subject-line to be used to open password protected attachments for mail sandboxing or should be able to configure password for manually uploaded files."
23	Page 45, Point 1.51	Endpoint advanced persistent threat component should have the option to send the file to sandbox for the analysis and take the action (Quarantine/Kill/Block) based on result	As per the scope of the RFP, we understand that NIC is looking for APT solution in integration with existing endpoint and network security solutions. Please confirm that this deployment modes can be achieved with integration with existing endpoint and network security solutions	As mentioned in the RFP bidder can propose solution integrating with the existing solution or standalone. If standalone solution is proposed then it should meet the minimum specification as mentioned in the RFP
24	Page 45, Point 1.52	The Proposed solution should be able to detect and analyze URLs which embedded in MS office, PDF attachments and in Email body for proposed mail sandboxing.	The body of the mail would have URLs which would be inspected by your existing web proxy or anti-spam solutions. Hence we would request you to please change the specs to "The Proposed solution should be able to detect and analyze URLs which embedded in MS office, PDF attachments and in Email body/attachment for proposed mail sandboxing."	As per RFP
25	Page 45, Point 1.53	The proposed solution detect and analyze the URL in the email subject proposed mail sandboxing.	The subject of the mail would have URLs which would be inspected by your existing web proxy or anti-spam solutions. Hence we would request you to please change the specs to "The proposed solution detect and analyze the URL in the email subject / attachment proposed mail sandboxing."	As per RFP
26	Page 45, Point 1.54	The Proposed solution should be able to Deliver the email message to the recipient after replacing the suspicious attachments with a text file and tag the email message subject with a string to notify the recipient	As per the scope of the RFP, we understand that NIC is looking for APT solution in integration with existing endpoint and network security solutions. Please confirm that this deployment modes can be achieved with integration with existing endpoint and network security solutions	As mentioned in the RFP bidder can propose solution integrating with the existing solution or standalone. If standalone solution is proposed then it should meet the minimum specification as mentioned in the RFP. Bidder to demonstrate how the same is achieved through integration
27	Page 46, Point 2.1	Network behaviour analysis component should have an automated discovery function to identify network devices and advanced persistent threat information such as IP address, OS, services provided, other connected hosts.	As per the scope of the RFP, we understand that NIC is looking for APT solution in integration with existing endpoint and network security solutions. Please confirm that this deployment modes can be achieved with integration with existing endpoint and network security solutions	As mentioned in the RFP bidder can propose solution integrating with the existing solution or standalone. If standalone solution is proposed then it should meet the minimum specification as mentioned in the RFP. Bidder to demonstrate how the same is achieved through integration
28	Page 46, Point 2.2	Should detect advanced persistent threat signature / heuristics based alerts and block the same	We understand that you are looking for APT solution integration with existing SIEM. Please confirm we SI can provide solution via that integration.	The bidder can provide the solution via integration as along as the network behaviour analysis component is able to create a baseline of the network and block infected host from connecting to the network

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
29	Page 46, Point 2.6	Should be capable of conducting protocol analysis to detect tunneled protocols, backdoors, the use of forbidden application protocols etc.	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	The network behaviour analysis component should have this functionality inbuilt to the solution
30	Page 46, Point 2.8	The solution should Integrate with Microsoft Active Directory, RADIUS, and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active Directory workgroup & Provides full historical mapping of User Name to IP address logins in a searchable format	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	As per RFP
31	Page 47, Point 2.9	Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantine VLANS	We understand that you are using Cisco ISE solution. This can be achieved via the same. Hence request you to remove this specs.	Network behaviour analysis component can be proposed with integration with Cisco ISE deployed in NIC Network, to achieve this functionality
32	Page 47, Point 2.11	Should support the capability to alert the admin and provide mitigation action like quarantine or block the endpoint or custom scripts like ACL push or block the further spread of the malware/worm while allowing legitimate traffic to continue	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	The bidder can provide the solution via integration as long as the required action is met. The action should be in a automated way and should not depend on the SOC team to take action manually

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
33	Page 47, Point 2.15	Should support the capability to link usernames to IP addresses for suspected security events	User behaviour analysis is a different solution than network behaviour analysis. Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	As per RFP
34	Page 47, Point 2.17	Should support the capability of Application profiling in the system and should also support custom applications present or acquired by the NIC	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	As per RFP
35	Page 47, Point 2.19	The solution should provide access to raw as well as processed logs	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	Network behaviour analysis component should provide statistic of the flows.
36	Page 47, Point 2.23	The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc.	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
37	Page 47, Point 2.26	The solution should support the identification of applications tunneling on other ports	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	As per RFP
38	Page 47, Point 2.28	The solution should be able to conduct de-duplication of redundant flow identified in the network to improve performance	This is specific to a particular OEM. Hence, would request you to kindly remove the same.	As per RFP
39	Page 47, Point 2.29	The solution should have the ability to state-fully reassemble unit-directional flows into bi-directional conversations; handling de-duplication of data and asymmetry	This is specific to a particular OEM. Hence, would request you to kindly remove the same.	As per RFP
40	Page 47, Point 2.30	The solution should support all forms of flows including but not limited to Cisco net flow, juniper flow, slow, infix for up etc.	Slow, Infix for Up are specific to a particular OEM. Kindly rephrase the clause to " 2.30 The solution should support all forms of flows including but not limited to Cisco net flow, juniper flow etc."	The solution should support cisco Netflow and juniper flow
41	Page 47, Point 2.31	The solution should be able to combine/stitch the flow records coming from different network devices like routers/switches/firewall that are associated with a single conversation and present them as a single bi-directional flow record	This is specific to a particular OEM. Hence, would request you to kindly remove the same.	As per RFP
42	Page 48, Point 2.32	The solution should be able to stitch flows into conversations even when the traffic is NATted by the firewall; clearly showing the original and translated IP address	This is specific to a particular OEM. Hence, would request you to kindly remove the same.	As per RFP
43	Page 48, Point 2.38	Should support both in line and offline modes.	Kindly clarify what is required in Inline Mode?	Should support inline or offline mode
44	Page 48, Point 2.41	For Devices / applications those do not support flows, the solution should be capable to generate its own flows for monitoring.	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	As per RFP
45	Page 48, Point 2.46	The solution should be deployed in HA between DC and DR.	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution.	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
46	3 GT&C - Price Schedule: Point B	All Inclusive Price of the Solution in respect of RFP/07/2017 will comprise of all Services, Hardware and accessories where applicable, license fees of all required software including OS licenses for 5 Years where applicable, On-Site Comprehensive Warranty (as per Specified Periods) where applicable, and should take into account price/charges as specified in the Commercial Bid, in respect of RFP/07/2017.	Please mention the start date for warranty. Will the start date be the date of delivery of the equipment or the date of implementation completion signoff?	Date of Implementation and completion sign-off of the individual components of the solution
47	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 4.2	The proposed component should be appliance based and purpose built for DDOS prevention and should be based on Load balancer/Firewall Architecture	We understand that NIC will require high performance architecture based product for DDOS detection and mitigation. Hence, the product should be purpose built and should not be based on load balancer/Firewall architecture. Our understanding is that there is a typo, "not" is missing. Request to amend this clause to "The proposed component should be appliance based and purpose built for DDOS prevention and should **not** be based on Load balancer/Firewall Architecture"	It should not be based on Load Balancer/Firewall.
48	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 4.21	The proposed solution must support cloud signaling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation	It is suggested that the cloud signaling to upstream ISP's should also be capable of informing the upstream ISP/Managed services provider of the victim's IP address and list of rogue IP's that are detected by the on-premise DDOS mitigation appliance. This feature would help seamless and effective mitigation handover to the cloud scrubbing center.	As per RFP
49	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 4.48	The proposed solution must support option for Centralized management of multiple devices in future.	Most of the DDOS mitigation appliance supports inbuilt management. Is it required to propose centralized management server for DDOS mitigation appliance at DC & DR?	Central Mangement is not needed now. But the support of the same should be available in the quoted devices and NIC will buy the additional devices when needed. Provide separate line-item as optional item for centralized management server. **Bidder to NOTE:** Bidder has to submit price for **ALL optional components**, but it will not be considered for L1 calculation i.e. selection of successful Bidder. However, successful Bidder will be asked to match the lowest price as discovered in this Optional Section, if NIC proceeds with the procurement of the Optional items as mentioned. Failure to quote will result in bid rejection.
50	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 4.81	The mitigation service must support GRE as clean traffic reinjection mechanism.	We understand that NIC has dual ISP connectivity at DC and DR. GRE tunneling would be required to deliver clean traffic from scrubbing centers to NIC DC/DR in the event of DDOS attacks. Will it require to provision redundant GRE tunnel at DC and DR for clean traffic re-injection?	Yes
51	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 4.118	On premise solution should be deployed in standalone mode in DC & DR. Currently NIC is having ip address provided the service provider and intends to shift to ip address from APNIC/IRINN	Please provide the details of APNIC/ARIN IP addresses space allocated to NIC. The details required are the number of /24 or /23 at DC and DR.	NIC is in the process of getting the APNIC/ARIN IP ip address and this will be not be bidder responsibility. However Bidder will help NIC in liaisioning with APNIC for the IP Addresses
52	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 5	All components of the Next Generation Threat Prevention solution should be in all locations as specified viz.DC, DR and HO; however the component of the Next Generation Threat Prevention solution, Serial Nos. 3.1 to 3.60 will not be required at HO.	As per our understanding the DDOS mitigation solution is required for DC and DR. It is not required for HO. Please confirm if the understanding is correct.	DC & DR only

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
53	Page 41 Clause No 26	Additional 5500 Licenses of Websense	NIC is currently using total 6600 numbers of license with single V10000 appliance at each location (i.e. HO, DC, DR). Single V10000 appliance is able to handle total 7500 numbers of user load. As per RFP NIC will procure additional 5500 licenses. After additional license procurement total number of user count will be 12100 and Forcepoint recommandation is: one more additional V10000 appliance is require at each location (i.e. HO, DC, DR) to handle the total user load. Kindly clarify whether the bidder should propose additional V10000 appliance	Addiitional Appliance not needed now. However, provide separate line-item as **optional component/item** for additional appliance
54	Page 41 Clause No 26	Additional 5500 Licenses of Websense	Forcepoint recommand to upgrade the Database server RAM from 16 GB to 32 GB.	Bidder to propose if the same is needed
55	Page 41 Clause No 26	Additional 5500 Licenses of Websense	Forcepoint query: Will this propose solution should meet the High Availability feature.	No
56	1.1 RFP /07/2107	The solution should be appliance-based solution	Privileged identity management is software based solution and not appliance based	The privileged identity management component can be software or appliance based
57	Additional Clause		1 As best practice for threat detection for Privilege accounts customer should look for must have functionality where privileged identity management help to detect indications of an attack such as lateral movement, credential theft and privilege escalation.	Accepted as additional feature, not mandatory
58	3.4 RFP //07/2017	The solution should be able to conduct session video recording for privileged users	Along with Session recoding As best practice for threat detection in session recording customer should look for must have functionality where privileged identity management component help to detect and terminate high Risk Sessions automatically .	Accepted as additional feature, not mandatory
59	3 GT&C - Price Schedule: Point B	All Inclusive Price of the Solution in respect of RFP/07/2017 will comprise of all Services, Hardware and accessories where applicable, license fees of all required software including OS licenses for 5 Years where applicable, On-Site Comprehensive	Please mention the start date for warranty. Will the start date be the date of delivery of the equipment or the date of implementation completion signoff?	Date of Implementation and completion sign-off of the individual components of the solution
60	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 4.21	The proposed solution must support cloud signaling to signal to upstream ISPs or managed service provider who is providing anti-DDoS cloud service for very large DDoS attack mitigation	It is suggested that the cloud signaling to upstream ISP's should also be capable of informing the upstream ISP/Managed services provider of the victim's IP address and list of rogue IP's that are detected by the on-premise DDOS mitigation appliance. This feature would help seamless and effective mitigation handover to the cloud scrubbing center.	As per RFP
61	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 4.81	The mitigation service must support GRE as clean traffic reinjection mechanism.	We understand that NIC has dual ISP connectivity at DC and DR. GRE tunneling would be required to deliver clean traffic from scrubbing centers to NIC DC/DR in the event of DDOS attacks. Will it require to provision redundant GRE tunnel at DC and DR for clean traffic re-injection?	Yes
62	63.5 Technical Compliance – Next Generation Threat Protection Solution. Point number 5	All components of the Next Generation Threat Prevention solution should be in all locations as specified viz.DC, DR and HO; however the component of the Next Generation Threat Prevention solution, Serial Nos. 3.1 to 3.60 will not be required at HO.	As per our understanding the DDOS mitigation solution is required for DC and DR. It is not required for HO. Please confirm if the understanding is correct.	DC &DR only
63	s 5	The Bidder should have at least 2 (Two) Information Security Orders of their National Customers, each having a order value of at least Rs. 10 Crores within the last 5 years Or, 4 (Two) Information Security Orders of their National Customers, each having a order value of at least Rs. 5 Crores within the last 5 years. Completion Certificates to be provided from Customer	We understand this is Security components clubbed in other order . Please confirm	Yes, Security components clubbed in other order is acceptable, as long as specific prices are shown to justify the criteria.

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017

NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM

DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
64	Page 48, Point 2.46	The solution should be deployed in HA between DC and DR.	Please confirm if SI can provide an option of achieving this requirement with integration with existing SIEM solution. Please provide the split of flows that would be captured from DC, DR and HO. Has NIC sized the WAN links for capturing flows from these 3 sites? What is the retention period expected for these flows? Would NIC provide storage space for these flows or does the SI has to qoute the stirage?	As per RFP; Retention period 1 year. Bidder to propose the solution with needed storage
65	17, 19 GT&C - Copyright violations and Patent Rights:	The Supplier shall indemnify 'NIC' in respect of all suits, action claims or damages arising out of violation of any Patents or Copyrights, for any and all components of the Solution supplied by the Supplier in respect of the RFP/07/2017. The Supplier shall indemnify 'NIC' against all third party claims of infringement of patent, trademark or industrial design rights arising from use of the goods and services, software package or any other part thereof in India.	Please replace the current clause with the following clause". In the event of a third party claim of intellectual property infringement, Bidder may, at its sole option, (i) obtain for Bank the right to continue using the Services, (ii) modify the services so that the services are non-infringing, (iii) replace the services with a functionally equivalent, non-infringing service, or (iv) if the alternatives in Section (i)-(iii) are not available, Bidder may so notify Customer and terminate such infringing Services without penalty to either Party. Notwithstanding anything in this Agreement to the contrary, this Section is Customer's sole and exclusive remedy for any intellectual property infringement claims."	As per RFP
66	17, 21 GT&C - Satisfactory Performance	The Supplier shall guarantee satisfactory performance of all hardware and software to the specifications in the Purchase Order and further undertake to reimburse the Purchaser in respect of all payments made in pursuance of this Purchase Order and such other cost as may be decided by mutual consent or by arbitrator, if the hardware / software features do not perform to committed standards thus materially affecting performance of the systems.	Bidder shall perform as per the techinical specification, the word unsatisfactory is ambiguous, therefore,please remove it, Customer shall be liable for liquidated damages and it should not be asked to pay compensation.	As per RFP
67	19, 31 (B)GT&C – Termination for Defaults	The Purchaser may, without prejudice to any other remedy for Breach of the Contract, by written notice of 30 days of default to the Bidder, terminate the Contract in respect of Volume-II in whole or in part; If the Supplier fails to perform any other obligations under the Contract	Termination should be only for the material breach of the contract.	As per RFP
68	21, 37 GT&C – Limitation of Liability	Supplier's aggregate liability for actual direct damages shall be limited to a maximum of the Contract Value, provided that this limit shall not apply to (1) the infringement indemnity; or (2) bodily injury (including death) and damage to real property and tangible personal property caused by Supplier's negligence. Supplier shall not in any event be liable for any indirect or consequential damages, or for loss of profit, business, revenue, goodwill, anticipated savings or data, or third party claims except with respect to bodily injury (including death) and damage to real and tangible personal property for which Supplier is legally liable. For the purposes of this Section, "Contract Value" at any given point in time, means the aggregate value of purchase orders placed by NIC on the Bidder under this project.	We propose the following clause to replace the current clause "NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL 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 THIS AGREEMENT, 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. IN NO EVENT BIDDER SHALL BE LIABLE IN AN AMOUNT THAT EXCEEDS, IN THE AGGREGATE FOR ALL SUCH LIABILITIES, THE MOST RECENT TWELVE (12) MONTHS OF CHARGES COLLECTED BY BIDDER FROM THE CUSTOMER PURSUANT TO THE APPLICABLE PURCHASE ORDER GIVING RISE TO THE LIABILITY. "	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
69	21, 41 GT&C – Indemnity:	The Supplier shall, at its own expense, defend and indemnify NIC against all third party claims for infringement of patent, trademark, design or copyright arising from use of products or any part thereof supplied by Supplier. Supplier will provide infringement remedies and indemnities for third party products, on a pass through basis. The Supplier shall expeditiously extinguish any such claims and shall have full rights to defend it there from. If NIC is required to pay compensation to a third party resulting from such infringement, the Supplier shall be fully responsible to pay such compensation along with all costs, damages and attorney's fees and other expenses that a court may finally awards, in the event of the matter being adjudicated by a court or that be included in a Supplier approved settlement. NIC will issue notice to the Supplier of any such claim without delay and provide reasonable assistance to the Supplier in disposal of such claim, and shall at no time admit to any liability for, or express any intent, to settle the claim. The Supplier shall also reimburse all incidental costs, which NIC incurs in this regard. In the event of the Supplier is not fulfilling its obligations under this clause within the period specified in the notice issued by NIC, NIC has the right to recover the amounts due to it under this provision from any amount payable to the Supplier under this project. The indemnities under this clause are in addition to and without prejudice to the indemnities given elsewhere in this agreement. In the event of the Supplier not fulfilling its obligations under this clause within the period specified in the notice issued by NiC, NIC has the right to recover the amounts due to it under this provision from any amount payable to the Supplier under this project. The indemnities under this clause are in addition to and without prejudice to the indemnities given elsewhere in this agreement.	We propose the following clause to replace the current clause "Each Party shall indemnify the other from and against any claims by third parties (including any Governmental Authority) and expenses (including legal fees and court costs) arising from damage to tangible property, personal injury or death caused by such Party's negligence or willful misconduct. NOTWITHSTANDING ANY OTHER PROVISION HEREOF, NEITHER PARTY SHALL 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 THIS AGREEMENT, 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. IN NO EVENT BIDDER SHALL BE LIABLE IN AN AMOUNT THAT EXCEEDS, IN THE AGGREGATE FOR ALL SUCH LIABILITIES, THE MOST RECENT TWELVE (12) MONTHS OF CHARGES COLLECTED BY BIDDER FROM THE CUSTOMER PURSUANT TO THE APPLICABLE PURCHASE ORDER GIVING RISE TO THE LIABILITY.	As per RFP
70	22, 46 GT&C - Termination for Convenience:	The Purchaser may by written notice of 60 days sent to the Supplier terminate the Contract, in whole or in part, any time for its convenience. The notice of termination shall specify that termination is for the Purchaser's convenience, the extent to which performance of work under the Contract is terminated and the date on which such termination becomes effective. The Purchaser may purchase the ordered goods that are complete and ready for installation after the Supplier's receipt of notice of termination at the Contract terms and prices. For the remaining goods and services, the Purchaser may elect: To have any portion completed and delivered at the contract terms and prices; and/or To cancel the remainder and pay to the supplier an agreed amount for partially completed goods and services and for materials and parts previously procured by the Supplier. All payments due to the Supplier till the effective date of termination may be made by NIC within 120 days' of such written notice for termination.	Termination for convineine shall cause hefty loss to the biddr, therefore, kindy remove the clause	As per RFP
71	41, 24	All documentations, but not limited to Design, Configuration etc. (HLD and LLD) must be handed over to NIC after successful implementation, commissioning and before release of final payment.	Bidder shall only provide only operational documents, no LLD, source code etc shall be provided to the bidder.	NIC does not require source code. NIC requires LLD, HLD related to configuration of the document and it's implementation, integration.

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
72	35, 5	The Bidder should have at least 2 (Two) Information Security Orders of their National Customers, each having a order value of at least Rs. 10 Crores within the last 5 years Or, 4 (Two) Information Security Orders of their National Customers, each having a order value of at least Rs. 5 Crores within the last 5 years Completion Certificates to be provided from Customer	Request NIC to please modify the clause as per below: The Bidder should have at least **1 (One)** Information Security Orders of their National Customers, each having a order value of at least Rs. 10 Crores within the last 5 years Or, 4 (Two) Information Security Orders of their National Customers, each having a order value of at least Rs. 5 Crores within the last 5 years Completion Certificates to be provided from Customer	As per RFP
73	35, 6	The Bidder should have implemented and maintained captive SOC for any two PSU/BFSI/Government customers (with at least 1000 locations) in India within last 3 years. SOC solution should have at least 4 out of the following components like SIEM, WAF, DAM, PIM, NBA, Anti-APT solutions/Anti-Phishing/DLP. Completion Certificates to be provided from Customer	Request NIC to please modify the clause as per below: The Bidder should have implemented and maintained captive SOC for any **one** PSU/BFSI/Government customers (with at least 1000 locations) in India within last 3 years. SOC solution should have at least 4 out of the following components like SIEM, WAF, DAM, PIM, NBA, Anti-APT solutions/Anti-Phishing/DLP, DDoS**.** Completion Certificates to be provided from Custo+E76mer	Clause modified as "The Bidder should have implemented and maintained captive SOC for any two PSU/BFSI/Government customers in India, (with one such customer having at least 1000 locations), within last 5 years. SOC solution should have at least 4 out of the following components like SIEM, WAF, DAM, PIM, NBA, Anti-APT solutions/Anti-Phishing/DLP in atleast one reference. Completion Certificates to be provided from Customer"
74	35, 7	The Bidder should have manpower with certifications in Information Security Operations. The Bidder should have at least 10 certified security professionals on their payroll with minimum two CISA/CISSP certifications	Request NIC to please modify the clause as per below: The Bidder should have at least **30** certified security professionals on their payroll with minimum **ten** CISA/CISSP certifications	As per RFP
75	40, 13, 14	Privileged Identity Management	Please provide the number of concurrent privileged users and the number of target devices in scope	Mentioned in RFP point 3.59
76	40, 21	The Supplier is responsible for integrating the solutions with the existing MacAfee SIEM.	Supplier can only facilitate integration of new technologies with existing SIEM by forwarding logs or configuring the system. The existing SIEM management team has to be primarily responsible for this integration	As per RFP
77	41, 26	Additonally, NIC requires the following as part of the solution delivery:	Bidder understands that this requirement is only limited to providing the technology components (HW, SW, Licences). The daily operations/management of these technologies will continue to be provided by the incumbent service provider.	As per RFP; RFP mentions Resources needed
78	57, 4.114	The service must have a dedicated Security Operations Center to provide mitigation support with 24x7 coverage.	The bidder must have atleast 3 Global SOCs, out of which 2 must be in India.	As per RFP
79	54, 4.65 - Technical Qualification	Cloud DDOS Service Provider shall have a purpose-built network of mitigation centers with at least 4Tb of mitigation capability.	Please clarifiy if this capacity required as the Global capacity or India specific capacity . Also , please change the clause to Ingestion capacity capablity	It can be India or Global
80	54, 4.71 - Technical Qualification	Cloud DDOS Service Provider should be able to detect and mitigate DDoS attacks from layer 3 to layer 7 of the OSI model in a distributed model where on-premise systems can interact with Cloud based mitigation infrastructure thru signaling. Please mention the detailed cloud signaling methodology	Please also add- Cloud DDOS Protection to handle all volumetric Layer 3 attacks and Inpremise to handle all Layer 7 attacks	Clause modified as follows: "Cloud DDOS Service Provider should be able to detect and mitigate DDoS attacks from layer 3 to layer 7 of the OSI model in a distributed model where on-premise systems can interact with Cloud based mitigation infrastructure thru signaling. Cloud DDOS Protection to handle all volumetric Layer 3 attacks and Inpremise to handle all Layer 7 attacks. Please mention the detailed cloud signaling methodology

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
81	54, 4.74 - Technical Qualification	Cloud DDOS Service Provider should have at-least 30% market share in on-premise /Cloud based DDOS market. Please provide adequate documents to support the compliance	Please clarify which document is required to validate this market share since there is no report available on cloud DDOS market	Third party market analysis report like Gartner, IDC, Forrester, Frost and Sullivan, Infonetic etc
82	55, 4.77 - Technical Qualification	DDOS mitigation service should provide 1 Gbps of clean traffic to DC/ DR. The service should be able to protect attack up-to 500 Gbps plus size. Size of attack traffic covered for NIC must be 500 Gbps plus. The service should protect both DC and DR	Please provide the details of the Internet Links and their capacities for the Clean Traffic perspective . Also, how is the additional clean pipe capacity shall be calculated once the pipe size increase beyond 1 gbps	Internet Links mentioned in the RFP. We don't need capacity beyond 1 Gbps
83	55, 4.85 - Technical Qualification	The mitigation service must have the ability to utilize NIC-provided certificates for decrypting SSL traffic in the cloud when using DNS re-direction	please remove the clause since SSL certificates can't be shared over cloud infra. Is DNS redirection protection required for the Website or any URL protection of NIC	This is optional.
84	55, 4.86 - Technical Qualification	The proposed solution should mitigate DDoS attacks from layer 3 to layer 7 of the OSI model.	Please modify this clause since cloud shall do layer 3 and Layer 7 on Premise based	Cloud protection will be for volumetric attacks and on premise solution for application attacks
85	55, 4.92 - Technical Qualification	The solution must include an on-premise component that is able to terminate GRE tunnels for reinjection of clean traffic from the cloud based mitigation centers. The on-premise component should comply to specification mentioned in the section "Technical specifications on-premise"	Please modify this clause since GRE Termination is recommended to be terminated on the Internet facing router	Bidder should provide the router if needed without additional cost to NIC
86	54, 4.66 - Technical Qualification	Cloud DDOS Service Provider shall describe its plans for expansion of mitigation capacity in order to withstand future forecasted size of attacks. Should provide roadmap to support at-least 50% upgradeability of mitigation capacity in next 1 year	NIC to elaborate what details are needed in the roadmap	Roadmap document should be shared to support the claim that the cloud DDOS service provider has plans to upgrade and enhance the mitigation capacity by 50% within next 1 year
87	54, 4.68 - Technical Qualification	Each mitigation center must connect to the Internet in a redundant way by making use of multiple different Internet providers. Please provide adequate details	Please let us in detail as to what details are required	Please provide the Scrubbing center architecture details like the upstream peering capacity, clean traffic links, scrubbing centers interconnects details etc.
88	54, 4.73 - Technical Qualification	Cloud DDOS Service Provider should be a qualified DDOS mitigation managed service provider. Should provide a written statement detailing the qualifications as DDoS mitigation managed service provider.	Please let us in detail as to what details are required	Any datasheet detailing the service offering provided
89	54, 4.75 - Technical Qualification	Cloud DDOS Service Provider should have good track record as a DDOS mitigation service provider. Please provide a synopsis of Cloud DDOS Service Provider track records and successes as DDoS mitigation service providers for the last three (3) years. The response must include information such as the approximate number of NICs and number of incidents successfully mitigated, industry recognition, expertise and research activities about DDoS, Botnets, Advanced Threats, etc.	Please elaborate in details on what NICs mean by?	Number of interface/ports. Please mention the approximate number of such on-premise appliance/NICs/Interfaces deployed
90	55, 4.83 - Technical Qualification	The platform must make use of stateless mitigation devices dedicated to DDoS mitigation (IDMS, Intelligent DDoS Mitigation Systems). Details to be provided	Please let us in detail as to what details are required	Mention the solution details of mitigation system deployed in the cloud for offering DDOS mitigation service. The details might include the products/technology/mechanism used
91	55, 4.84 - Technical Qualification	In addition to IDMSs, the platform must provide the ability to integrate additional mitigation techniques. Details to be provided	Please let us in detail as to what details are required	Cloud DDOS service provider is expected to deploy techniques like RTBH, Flowspec, ACL and other Router level control plane mechanism to block high volume DDOS attacks, in addition to the Intelligent DDOS mitigation systems. Please provide details

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
92	56, 4.106- SLAs AND REPORTING & Operational Support	The service must provide a measurable Time to mitigate SLA under 15 minutes	Request NIC to increase the Time to Mitigate SLA framework to Industry Standard acceptable timelines such as 30 minutes	As per RFP
93	56, 4.107- SLAs AND REPORTING & Operational Support	The service must provide a measurable Time to mitigate SLA under 5 minutes for volumetric attacks	Request NIC to increase the Time to Mitigate SLA framework to Industry Standard acceptable timelines such as 30 minutes	As per RFP
94	56, 4.108- SLAs AND REPORTING & Operational Support	The Cloud DDOS Service Provider must guarantee that service is set up within 3 days from receipt of provisioning information.	Request NIC to increase the timeframe to 7 working days	As per RFP
95	56, 4.109- SLAs AND REPORTING & Operational Support	The service must provide an emergency setup option for DNS based diversion within 4 hours from receipt of purchase order	NIC to elaborate on the DNS Based diversion required technically	If NIC intends to add additional url for protection which is not under the scope it is expected to make the protection within the time mentioned
96		GENERIC QUERY TO SIZE THE CLOUD ANTI DDOS SOLUTION	All links that needs DDoS Protection are connected with tata backbone or Other ISP links ? Number of Locations / Sites that needs DDoS Protection?- This helps to determine number of DDoS Profiles. Number of IP Subnets to Be protected ?- IPV4/ IPV6 and also mention the number of segments?(eg:One /24 IPV4) In case if customer has TATA Links, Are customer's IP Addresses that needs DDoS Protection advertised on TATA Backbone only? In case if customer has Non-TATA Links/Non-TATA ISP , Does customer own the Public IP? Does customer has IP Pools advertised on Non-TATA Links /ISPs greater than /24 ? Does customer has an Own AS? In case of OFFNET, What are the number of OFFNET Edge routers from which netflow information needs to be exported for detecting DDoS Attacks on OFFNET Links? What are the no. of GRE Tunnels ? What are the No. of OFFNET routers from where the Netflow information is to	Will be provided to the successful bidder
97		GENERIC QUERY	Request NIC to provide details on the existing Network Architechture where the Anti-DDDoS Solution has to be deployed	Will be provided to the successful bidder
98	50, 3.45	The solution should have the ability to control where a privileged user can access a device/application on the basis of IP addresses.	Do NIC have any or bidder has to provide the same with the fetures mentioned in the RFP. Please clarify.	Bidder to provide the privileged identity management component

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
99	71, Table B: Software Cost	Approx. 2000 thousand Forti Mobile Token to run Two Factor Authentication for VPN Users (Fortinet Local users + AD users) 5500 licenses of Websense Additional 2000 licenses of McAfee Endpoint Encryption Trend Micro Deep Security licenses - 100	Understand NIC is having existing two factor authentication, Websense proxy , MCAfee endpoint encrypyion and Trend Micro deep security. Do the bidder need to supply additional licenses only and the existing solution to be managed by NIC only. Please clarify the same.	License only
100	71, Table C- Manpower	L3 On-Site SOC Engineer L1 On-Site SOC Engineer	2 x L3 and 2 x L1 Engineers asked in the RFP. Is this only for Anti APT, DDoS and PIM. Please clarify.	It is for all solutions mentioned in the RFP
101	42, 63.5 Technical Compliance – Next Generation Threat Protection Solution	The solution should be appliance-based solution	The volumentric DDoS mitigation is recommended to be on cloud as the nature of the attack is to flood the network. Hope this can be provided on cloud please let us know.	This is for Anti APT compliance and not for DDOS.It can be appliance or vm appliance
102	48, 2.34	The solution should be able to integrate with various SIEMs available in the market like RSA, Splunk, HP, McAfee Nitro etc. NIC uses McAfee Nitro, solution should integrate with mentioned SIEM	The solution should be integrated with existing McAfee Nitro SIEM and NIC to take care of the additional EPS count and sources along with log retention and corelation capabilities of existing SIEM solution. Bidder will not be managing the existing SIEM solution. Is our understanding correct please let us know.	SIEM will be managed by existing SI at NIC.Bidder should integrate the proposed solutions with the SIEM. Bidder shall also be responsible for provisioning and integration with SIEM whenever any such custom plugin needed; during the entire life-time of the project, at no extra cost.
103	48, 2.46	The solution should be deployed in HA between DC and DR.	High Availablity required in both DC and DR or standalone deployment in DC and DR and HA between DC and DR solution is required. Please clarify.	HA can be proposed across D-DR with primary at DC and standby at DR
104	57, 4.118	On premise solution should be deployed in standalone mode in DC & DR. Currently NIC is having ip address provided the service provider and intends to shift to ip address from APNIC/IRINN	If NIC goes for IP pools from APNIC/IRINN with public ASN then it is evident that NIC will change the IP routes during a voumetric DDOS attack to the cloud DDOS mitigation servise provider for cleaning of traffick.	Yes
105	50, 3.57	The solution should be able to integrate with vulnerability management solution to ensure that automated VA scans utilize privileged accounts for devices which are managed by the PIM solution	Do NIC is having existing VA scan solution that needs to be integrated. Or bidder has to provide VA scan solutions then please let us know the detailed specifications required for VA scanning.	No VA solution asked in the RFP
106		GENERIC QUERY	Request NIC to provide details on the existing Network Architechture where the Anti-DDDoS Solution has to be deployed	Will be provided to the successful bidder
107	63, 39	63 Scope of Work	Proposed Next Gen Threat Protection Solution should have the following capabilities: Should have central management covering web (including VPN), email and endpoint Proposed solution should have ability to detect advanced targeted threats by leveraging, revamping the existing technologies already deployed. If any other solution is proposed then the bidder has to propose solution which integrates by sharing threat intelligence in real time with the existing Endpoint and Network security solutions. *If bidder proposes new solution then the new solution has to be proposed for total of 5 years, which will start after expiry of the license available for existing endpoint and network security solutions.* Need clarity on the clause - (After expiry of the license available for exisitng endoint.) What is the expiry of the existing endpoint license. What is the expected scope till the time the existing license is available.	Validity of existing endpoint and server licenses are for another period of 2 years approximately. In case of new solution, the solution should not have any dependency on existing end-point AV products and Bidder should ensure that both the solutions co-exist.

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
108	39, 63	Proposed Next Gen Threat Protection Solution should have the following capabilities: Should know the list of know bad talkers, whom they talk to, so attacks can be stopped even before they happen. In most ransomware and similar next-gen malware attacks, the Domain Name System (DNS) is used to resolve the IP address which is the command and control for the malware, known as C2. Solution should have information on DNS, new registrants of Domain Names, history of registrant and domain name behavior, with whom the IPs are communicating, to be able to stop the threat before it becomes an issue.	Need clarity on the requirement - The mailcious IP, Domains, URL are can be made available to all Anti-APT vendor solution using the Threat Intel feed integrated with that solution. DNS solution is not required explicitly to integrate the solution since it is a overhead. It may lead to favor to one specific OEM.	DNS solution not required
109	39, 63	Proposed solution should be on premise solution and should work without any dependency on cloud for sandboxing technology.	Need clarity on the OS support required for the Sandboxing for customer enduser enviornment.	Windows7, Windows 8, Windows 10 and its versions
110	39, 63	The components of the proposed solution should provide comprehensive 360 degree view of the network from endpoint to the exit to correlate patterns of malicious behaviour (discovering and monitoring traffic across the network and endpoint).	Need change in the clause - The 360 degree view should include Network, Email, Web, Server DC & DR and Endpoint. Since when we the cyber kill chain the hackers not only target the endpoints, they are going after the critical data which are in DC & DR and they escalate previleges inside DC & DR on critical servers. So the visibility of 360 degree should not be restricted to only network and endpoint allowing to integrate with existing solution in DC &DR.	As per RFP
111	39, 63	Proposed solution should monitor, analyse and record all file activity on a system, regardless of a file's posture at inception. If at a later date a file behaves suspiciously, solution should **retrospectively alert**, quarantine/remediate.	The clause should be generic and it is calling out specific feature of one OEM product.	These are expectations from the solution. The bidder should propose based on the techincal parameters
112	39, 63	Should record detailed history and trajectory of the malware including point and technique of entry to the network, locations where it resides and current activity across all such locations.	Solution should not only restricted to network and end point. Since the hacker will get point of entry to customer infra irrespective of the location. The solution should protect all infra, DC, DR, endpoint and should coexist with existing solutions in DC & DR.	As per RFP
113	39, 63	The Supplier is responsible for integrating the solutions with the existing MacAfee SIEM. Any customization needed for the same will be Supplier's responsibility	Need clarity on the scope - The SIEM integration should be part of the existing SIEM managed Service partner. The Nextgen threat RFP bidder can work with exiting SIEM parter and provide inputs and any support required. Since if the proposed OEM are not a standard data source, the SIEM partner need to develope the custom plugin for the new OEM. Which is can be done only by the existing SIEM partner who has all control and license to develope the new plugin.	Bidder shall also be responsible for provisioning and integration with SIEM whenever any such custom plugin needed; during the entire life-time of the project, at no extra cost.
114	41, 63	26. Additonally, NIC requires the following as part of the solution delivery: Approx. 2000 thousands Forti Mobile Token to run Two Factor Authentication for VPN Users (Fortinet Local users + AD users) Additional 5500 Licenses of Websense Additional 2000 licenses of McAfee Endpoint Encryption 10G Multimode SFP Module for existing NIC DC & DR 1500D Fortinet Firewall Box to meet their upcoming requirement (Total Qty. = 16). Four 1Gig Multimode SFP Module for existing NIC DC & DR Forti Authenticator 3000D Box (Total Qty = 4) to meet upcoming requirements. Additional 100 licenses of Trend Micro Deep Security	Need clarity on the scope of additional license requirement. The requirement is to only supply additional licesne. The service level, integration, management and warranty clause may not applicable to the commponents those are supplied under additional requirement. Please confirm.	Scope includes supply of license only
115	42, 63	The proposed network advanced persistent threat component should have the ability to be deployed in the following modes: Out of -band mode Iinline monitoring mode Inline active blocking mode	Request change the caluse, the solution should be integrated to make of existing IPS, Firewall and and block any C2 or malicious communication.	Bidder can propose by integrating with the existing solution as mentioned in the RFP. The same should work in case NIC changes in future

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
116	44, 63	The solution must be able to detect and report malware by using multiple operating systems ((like: Windows 7, Windows 8/8.1, Windows 10, Windows Server 2003/2008/2012/2016) (with multiple service pack levels) supporting both 32-bit and 64-bit architectures. The OS licenses are to be provided by the bidder along with the appliance	Please confirm there are the OS support require for Sandboxing. Will the OS coveres all enduser scenarios?	Yes
117	General	Endpoint ,Email Gateway Web Gateway, DC & DR Advanced Server Security Suite Integration with Anti-APT solution	Please support us with the details on the Different Internet breakout available to NIC. Does customer have the Forcepoint Web Security Gateway in all the locations where the Internet breakout or it is central internet breakout.	All locations. DC,DR & HO
118	46, 63	Network behaviour analysis component should have an automated discovery function to identify network devices and advanced persistent threat information such as IP address, OS, services provided, other connected hosts.	Request to clarify the scope for Network behaviour analysis component. Customer already having the Deep secutity solution which controls the EAST to West in Data Center enviornment can provide the malicious communication in DC & DR.	Network behaviour analysis component scope is different from what Deep security provides. It will cover,DC,DR,HO and branches
119	4, 1.5 (C)	The Bidder should be agreeable to hold the price and configuration for a period of at least one year from the date of opening of Commercial Bid in respect of his bid under the RFP, and in case there occurs any change in the specifications on account of the Solution offered/ordered for being phased out from the market, should be able to supply solution and systems of higher configuration at the same prices agreed to, in respect of the bid under the RFP as in Volume-II.	Tata Communication requests NIC to update the bid validity from 1 year to 90 days.	As per RFP
120	10, 3 (J)	The Supplier shall agree to maintain the price and configuration of all the components supplied in respect of RFP/07/2017 under this document for one (1) year from the date of opening of the Commercial Bid. However, should there be a fall in the prices between the date of submission of bid and the date of delivery of the Solution ordered for in respect of RFP/07/2017, on account of revision in prices in Services, Hardware / Software and any other components or on account of revision in duties and taxes or for any other reason whatsoever, the benefit shall be passed on to NIC. Similarly, if model of any product related to the Solution ordered for in respect of the RFP is replaced in the market by models of better technology or configuration before it is delivered, delivery should be of the latest configuration / technology without any price implication.	Tata Communication requests NIC to update the bid validity from 1 year to 90 days.	As per RFP
121	18, 28	Penalty: Non-compliance of the SLA as per the Table No-1, Sl.No.1, penalty would be Rs. 10,000/- per device per day for each day or part thereof, for device not functioning as per specifications (all days of the week). The overall penalty cap would be 15% of the respective component cost of the Next Generation Threat Prevention Solution. After the cap is reached, NIC may cancel the contract.	Tata Communication requests NIC to update the capping from 15% to 5% of respective component.	As per RFP
122	19, 28	Liquidated Damages: If the Supplier fails to Deliver within scheduled period, 'NIC' shall deduct from the contract price, as liquidated damages, a sum equivalent to 0.50% of the price of the delayed goods for each week (7 days) or part thereof of delay until actual delivery, up to a maximum deduction of 10% of the value of the delayed goods. Once such delay crosses the maximum limit, 'NIC' may consider contract either full and/or, in part, and annulment of order, either full and/or, in part.	Tata Communication requests NIC to update LD from 0.50% to 0.10% of price of delayed goods for each week.	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
123	19, 29	May procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered and/or not performed, and the Supplier shall be liable to the Purchaser, for any excess costs upto a maximum value of 10% of the Contract Value, for such similar Services. However, the Bidder shall continue performance of the Contract to the extent not terminated	Tata Communication requests NIC to remove this clause as there is already a penalty associated with the non-delivery.	As per RFP
124	General - Infrastructure	General	Please let us know if there is any plan for Private/Public/Hybrid Cloud incorporation	No
125	General - Infrastructure	General	Please let us know the failover mechanism for DC and DR and if the security infrastructure is exactly same	Bidder to propose the failover mechanism for the proposed solutions
126	63 - Scope of Work	Should have central management covering web (including VPN), email and endpoint Proposed solution should have ability …. which will start after expiry of the license available for existing endpoint and network security solutions.	Please let us know the current security control mechanism to manage all security products from same console, if implemented	RFP states the proposed solution should have central management
127	General - Infrastructure	General	Please mention if there is any audit in place for firewalls currently	No. The RFP doesn't ask for this
128	63.5 - Technical Compliance	Section 4.2	Please mention the technology utilised to load balance between servers and between DC-DR. Kindly mention if there is an external load balancer utilised for the same.	Bidder to factor load balancer as part of the solution
129	General - Infrastructure	General	Please mention if there is any access control solution implemented for providing varying level of access to different group of users and if any profiling has been configured for users	Cisco ISE solution is currently in place
130	General - Infrastructure	General	Please mention any Anti APT solution deployed at NICL.	The RFP is for Next Generation Threat Prevention including advanced persistent threats
131	General - Infrastructure	General	Please provide the details of the solution already integrated with McAfee SIEM. Also please confirm what are the solutions under the scope of SIEM integration.	The solution proposed as part of the RFP should be integrated with SIEM
132	General - Infrastructure	General	Please provide details of current SIEM and Anti APT solution Architecture	Details available in RFP
133	4 F	EMD - The EMD will be forfeited if the successful Bidder refuses to accept purchase order or having accepted purchase order fails to carry out his obligations mentioned therein. Additionally, such bidder will be blacklisted and barred from participating in any future RFPs' of NIC.	The EMD will be forfeited if the successful Bidder refuses to accept purchase order or having accepted purchase order fails to carry out his obligations mentioned therein **due to reasons solely attributable to the Bidder and Despite adequeate consideration of Bidder's deviations by NIC**. ~~Additionally, such bidder will be blacklisted and barred from participating in any future RFPs' of NIC.~~	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
134	10 J	The Supplier shall agree to maintain the price and configuration of all the components supplied in respect of RFP/07/2017 under this document for one (1) year from the date of opening of the Commercial Bid. However, should there be a fall in the prices between the date of submission of bid and the date of delivery of the Solution ordered for in respect of RFP/07/2017, on account of revision in prices in Services, Hardware / Software and any other components or on account of revision in duties and taxes or for any other reason whatsoever, the benefit shall be passed on to NIC. Similarly, if model of any product related to the Solution ordered for in respect of the RFP is replaced in the market by models of better technology or configuration before it is delivered, delivery should be of the latest configuration / technology without any price implication.	The Supplier shall agree to maintain the price and configuration of all the components supplied in respect of RFP/07/2017 under this document for one (1) year from the date of opening of the Commercial Bid. However, should there be a fall in the prices between the date of submission of bid and the date of delivery of the Solution ordered for in respect of RFP/07/2017, on account of revision in prices in Services, Hardware / Software and any other components or on account of revision in duties and taxes or for any other reason whatsoever, **upon mutual agreement between the parties,** the benefit shall be passed on to NIC. ~~Similarly, if model of any product related to the Solution ordered for in respect of the RFP is replaced in the market by models of better technology or configuration before it is delivered, delivery should be of the latest configuration / technology without any price implication.~~	As per RFP
135	11 B	The Bidder should enclose a Letter of Authority in favour of 'NIC' from the original manufacturers (MAF) as per format provided, and where required as per the RFP conditions.		As per RFP
136	13 8	Delivery Schedule - As per RFP		As per RFP
137	14 11	Terms of Payment: - As per RFP	**All payments shall be made within 30 days' of submission of invoices**	As per RFP
138	15 13	Payment will be made in the following Manner: Installation, Integration and Commissioning of Next Generation Threat Protection Solution --- Payment Terms : Remaining Cost of respective Hardware / Software / Licenses / all other accessories related to Installation, Integration and Commissioning.	we request NIC to change the clause to following : Remaining Cost of respective Hardware / Software / Licenses / all other accessories related to Installation, Integration and Commissioning OR submission of Bank Guarantee of equal amount with validity of one year.	As per RFP
139	15 14	Documents to be produced for the release of payment: - As per RFP		As per RFP
140	15 15	Availability of Product and Spares - As per RFP		As per RFP
141	16 16	Warranties - As per RFP		As per RFP
142	16 17	Guarantee - As per RFP	Request to delete. Everything to be covered under waranties	As per RFP
143	16 18	Maintenance during Warranty and AMC Period - As per RFP		As per RFP
144	17 21	Satisfactory Performance - The Supplier shall guarantee satisfactory performance of all hardware and software to the specifications in the Purchase Order and further undertake to reimburse the Purchaser in respect of all payments made in pursuance of this Purchase Order and such other cost as may be decided by mutual consent or by arbitrator, if the hardware / software features do not perform to committed standards thus materially affecting performance of the systems.	The Supplier shall ~~guarantee~~**ensure** satisfactory performance of all hardware and software to the specifications in the Purchase Order ~~and further undertake to reimburse the Purchaser in respect of all payments made in pursuance of this Purchase Order and such other cost as may be decided by mutual consent or by arbitrator, if the hardware / software features do not perform to committed standards thus materially affecting performance of the systems~~.	As per RFP
145	17 24	Change of purchase order - 'NIC' may at any time, by written order to the Supplier, make changes within the general scope of the Purchase Order. NIC will be free to either reduce or increase the quantity/configuration/specifications of the items to be purchased/change place of delivery or installation, on the same terms and conditions. NIC also reserves the right to place repeat orders for upto 25% quantity on any item, subject to Section-12, within 24 months of the date of the Purchase Order.	'NIC' may at any time, ~~by written order to~~**upon mutual agreement with** the Supplier, make changes within the general scope of the Purchase Order. NIC will be free to either reduce or increase the quantity/configuration/specifications of the items to be purchased/change place of delivery or installation, on the same terms and conditions. NIC also reserves the right to place repeat orders for upto ~~25~~**10**% quantity on any item, subject to Section-12, within 24 months of the date of the Purchase Order.	As per RFP

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
146	18 26	Cancellation clause - As per RFP	Request cure period of thirty days. Request add the following, "**Either Party shall have the right to terminate this Agreement at any time in the event that the other party commits a material breach of the Agreement and fails to cure such default to the non-defaulting party's reasonable satisfaction within thirty (30) days.** **In any event of termination, the Bidder shall be paid for the:** **1. goods delivered** **2. services rendered** **3. work in progress** **4. unpaid AMCs** **5. third party orders in pipeline which cannot be cancelled despite Bidder's best efforts** **5. unrecovered investments shall be paid by customer as per termination schedule till the date of termination.**"	As per RFP
147	18 27	Delay in Supplier's performance - As per RFP		As per RFP
148	19, 28, LD	As per RFP	Maximum aggregate LD under this RFP to be capped at 3% of the defaulting/delaed deliverables.	As per RFP
149	19, 29, Resort to LD	May procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered and/or not performed, and the Supplier shall be liable to the Purchaser, for any excess costs upto a maximum value of 10% of the Contract Value, for such similar Services. However, the Bidder shall continue performance of the Contract to the extent not terminated.	May procure, upon such terms and in such manner as it deems appropriate, services similar to those undelivered and/or not performed, and the Supplier shall be liable to the Purchaser, for any excess costs upto a maximum value of ~~10~~**3**% of the Contract Value, for such similar Services. However, the Bidder shall continue performance of the Contract to the extent not terminated.	As per RFP
150	20, 31, Termination for Defaults	A If the Supplier fails to render services within the time period(s) specified in the Contract or any extension period thereof granted by the Purchaser, or B If the Supplier fails to perform any other obligations under the Contract RFP Number – RFP/07/2017 C All payments due to the Supplier till the effective date of termination may be made by NIC within 60 days' of such written notice of termination, subject to applicable penalties, Section - 29.	A If the Supplier fails to render services within the time period(s) specified in the Contract or any extension period thereof granted by the Purchaser, or B If the Supplier fails to perform any other obligations under the Contract C All payments due to the Supplier till the effective date of termination may be made by NIC within ~~60~~ **30** days' of such written notice of termination~~, subject to applicable penalties, Section - 29.~~	As per RFP
151	20, 35, Contract with NIC	As per RFP	The successful Bidder will have to enter into a contract with National Insurance Company Ltd. within 15 working days of **mutual agreement between theparties on the terms and conditions and** issue of Purchase Order in respect of RFP/07/2017. The format of the Contract is attached in Volume-I. Failure to enter into Contract may result in cancellation of the Purchase Order/s and forfeiture of EMD/PBG.	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017

NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM

DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
152	21, 37, Limitation of Liability	Supplier’s aggregate liability for actual direct damages shall be limited to a maximum of the Contract Value, provided that this limit shall not apply to (1) the infringement indemnity; or (2) bodily injury (including death) and damage to real property and tangible personal property caused by Supplier’s negligence. Supplier shall not in any event be liable for any indirect or consequential damages, or for loss of profit, business, revenue, goodwill, anticipated savings or data, or third party claims except with respect to bodily injury (including death) and damage to real and tangible personal property for which Supplier is legally liable. For the purposes of this Section, “Contract Value” at any given point in time, means the aggregate value of purchase orders placed by NIC on the Bidder under this project.	**Notwithstadning anything to the contrary,** Supplier’s aggregate liability for actual direct damages**, for all claims including claims for indemnification,** shall be limited to a maximum of the Contract Value, provided that this limit shall not apply to (1) the infringement indemnity; or (2) bodily injury (including death) and damage to real property and tangible personal property caused by Supplier’s negligence. Supplier shall not in any event be liable for any indirect or consequential damages, or for loss of profit, business, revenue, goodwill, anticipated savings or data, or third party claims except with respect to bodily injury (including death) and damage to real and tangible personal property for which Supplier is legally liable. For the purposes of this Section, “Contract Value” at any given point in time, means the ~~aggregate~~**annual** value of **the applicable** purchase order~~s~~ placed by NIC on the Bidder under this project **under which the claim arises**.	As per RFP
153	22, 41, Indemnity	As per RFP	Request to add the following, " Bidder shall not have any liability to Customer under this Section to the extent that any infringement or claim thereof is attributable to: (1) the combination, operation or use of a Deliverable with equipment or software supplied by Customer where the Deliverable would not itself be infringing; (2) compliance with designs, specifications or instructions provided by Customer; (3) use of a Deliverable in an application or environment for which it was not designed or contemplated under this Agreement; or (4) modifications of a Deliverable by anyone other than Bidder where the unmodified version of the Deliverable would not have been infringing. Bidder will completely satisfy its obligations hereunder if, after receiving notice of a claim, Bidder obtains for Customer the right to continue using such Deliverables as provided without infringement, or replace or modify such Deliverables so that they become non-infringing."	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017

NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM

DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
154	22, 46, Termination for Convenience	A The Purchaser may by written notice of 60 days sent to the Supplier terminate the Contract, in whole or in part, any time for its convenience. The notice of termination shall specify that termination is for the Purchaser’s convenience, the extent to which performance of work under the Contract is terminated and the date on which such termination becomes effective. B The Purchaser may purchase the ordered goods that are complete and ready for installation after the Supplier’s receipt of notice of termination at the Contract terms and prices. For the remaining goods and services, the Purchaser may elect: B.1 To have any portion completed and delivered at the contract terms and prices; and/or B.2 To cancel the remainder and pay to the supplier an agreed amount for partially completed goods and services and for materials and parts previously procured by the Supplier. B.3 All payments due to the Supplier till the effective date of termination may be made by NIC within 120 days' of such written notice for termination.	A The Purchaser may by written notice of ~~60~~**90** days sent to the Supplier terminate the Contract, in whole or in part, any time for its convenience. The notice of termination shall specify that termination is for the Purchaser’s convenience, the extent to which performance of work under the Contract is terminated and the date on which such termination becomes effective. B The Purchaser may purchase the ordered goods that are complete and ready for installation after the Supplier’s receipt of notice of termination at the Contract terms and prices. For the remaining goods and services, the Purchaser may elect: B.1 To have any portion completed and delivered at the contract terms and prices; and/or B.2 To cancel the remainder and pay to the supplier an agreed amount for partially completed goods and services and for materials and parts previously procured by the Supplier. B.3 All payments due to the Supplier till the effective date of termination may be made by NIC within ~~120~~**30** days' of such written notice for termination.	Clause modified to 90 days.
155	23, 48, Compliance with Terms and Conditions	The Bidder will comply with all the terms and conditions given in this Master Document and RFP/07/2017.	The Bidder will comply with all the terms and conditions given in this Master Document and RFP/07/2017**, subject to the provided deviations**.	As per RFP
156	23, 51, Compliance with NIC's Information Security Policies	Prior to Supplier deploying any of it Personnel or engaging any person to perform Services for NIC; the Supplier shall, at a minimum, with respect to each such Personnel comply with NIC’s Information security policy/ies (ISP/s), as may be amended from time to time. Supplier hereby acknowledges that it has received a copy of the current ISP/s simultaneously with the execution of this Agreement. Supplier shall not assign any Personnel to perform the Services under this Agreement who does not comply with the provisions of the ISP/s. NIC shall have the right to audit Supplier’s books and records/facilities / location / places prepared or kept in connection with the Services at all reasonable times and places to ensure compliance with the ISP/s, to the extent applicable.	Prior to Supplier deploying any of it Personnel or engaging any person to perform Services for NIC; the Supplier shall, at a minimum, with respect to each such Personnel comply with NIC’s Information security policy/ies (ISP/s), as may be amended from time to time. Supplier hereby acknowledges that it has received a copy of the current ISP/s simultaneously with the execution of this Agreement. Supplier shall not assign any Personnel to perform the Services under this Agreement who does not comply with the provisions of the ISP/s. **Upon providing a notice period fo 30 days, during normal business hours and not more that once every financial year,** NIC shall have the right to audit Supplier’s books and records/facilities / location / places prepared or kept in connection with the Services at all reasonable times ~~and places~~ to ensure compliance with the ISP/s, to the extent applicable**, provided, however, that, such audits shall exclude any internal cost records, in any case**.	As per RFP
157	35	In the event of default by the Bidder with respect to this RFP or the Master Document, NIC may debar the Bidder from participating in any future RFPs’ floated by NIC for any purpose.	~~In the event of default by the Bidder with respect to this RFP or the Master Document, NIC may debar the Bidder from participating in any future RFPs’ floated by NIC for any purpose.~~	As per RFP
158	67, 68	We have carefully read and understood the terms and conditions of the Master Document and RFP/07/2017 and the conditions of the Contract applicable to the bid and we do hereby undertake to provide services as per these terms and conditions.	We have carefully read and understood the terms and conditions of the Master Document and RFP/07/2017 and the conditions of the Contract applicable to the bid and we do hereby undertake to provide services as per these terms and conditions **as read together with our deviations**.	As per RFP

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
159	Intellectual Protection	Clause not present in RFP	No intellectual property rights of any nature shall be transferred from one party to the other in the course of performing any obligations or otherwise under this agreement. For the avoidance of doubt, Bidder may use certain tools, processes or methodologies of its own in performing the Services. Ownership of all intellectual property rights and any other rights in these shall vest with Bidder, and no rights shall be deemed to have accrued to the Customer.	As per RFP
160	SNR	Clause not present in RFP	Customer hereby agrees to make the site ready as per the agreed specifications, within the agreed timelines. Customer agrees that Wipro shall not be in any manner be liable for any delay arising out of Customer's failure to make the site ready within the stipulated period, including but not limited to levy of liquidated damages for any delay in performance of Services under the terms of this Agreement. In case the SITE is not ready for a continious period of 30 days, milestone payment related to installation will be released to vendor based on the SNR report, also if there is any additional warranty cost due to continious site not readiness for 30 days, same will be borne by the customer	As per RFP
161	Risk and Title	Clause not present in RFP	Notwithstanding anything to the contrary contained elsewhere in the contract, The risk, title and ownership of the products shall be transferred to the customer upon delivery of such products to the customer	As per RFP
162	Deemed Acceptance	Clause not present in RFP	Products/Services and/or deliverables shall be deemed to be fully and finally accepted by Customer in the event when Customer has not submitted its acceptance or rejection response in writing to Wipro within 15 days from the date of installation/commissioning or when Customer uses the Deliverable in its business, whichever occurs earlier. Parties agree that Wipro shall have 15 days time to correct in case of any rejection by Customer.	As per RFP
163	Pass Through Warranty	Clause not present in RFP	Wipro shall “pass-through” any and all warranties and indemnities received from the manufacturer or licensor of the products and, to the extent, granted by such manufacturer or licensor, the Customer shall be the beneficiary of such manufacturer’s or licensor’s warranties and indemnities. Further, it is clarified that Wipro shall not provide any additional warranties and indemnities with respect such products.	As per RFP
164	ERV	Clause not present in RFP	“It is agreed that the price quoted is arrived at based on the exchange rate of 1 USD = INR ___ (“Base Exchange Rate”). In the event the Base Exchange Rate either increases or decreases by percentage points greater than two per cent [2%], the prices shall be charged as per the then current exchange rate.”	As per RFP

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
165	Non Hire Clause	Clause not present in RFP	Customer acknowledges that personnel to be provided by Wipro represent a significant investment in recruitment and training, the loss of which would be detrimental to Wipro’s business. In consideration of the foregoing, Customer agrees that for the term of this Agreement and for a period of one year thereafter, Customer will not directly or indirectly, recruit, hire, employ, engage, or discuss employment with any Wipro employee, or induce any such individual to leave the employ of Wipro. For purposes of this clause, a Wipro employee means any employee or person who has who has been involved in providing services under this Agreement.	As per RFP
166	Saving Clause	Clause not present in RFP	Wipro’s failure to perform its contractual responsibilities, to perform the services, or to meet agreed service levels shall be excused if and to the extent Wipro performance is effected , delayed or causes non-performance due to Customer's omissions or actions whatsoever.	As per RFP
167	Change Order	Clause not present in RFP	Either party may request a change order (“Change Order”) in the event of actual or anticipated change(s) to the agreed scope, Services, Deliverables, schedule, or any other aspect of the Statement of Work/Purchase Order. Wipro will prepare a Change Order reflecting the proposed changes, including the impact on the Deliverables, schedule, and fee. In the absence of a signed Change Order, Wipro shall not be bound to perform any additional services.	As per RFP
168	Termination for default	Clause not present in RFP	Either Party shall have the right to terminate this Agreement at any time in the event that the other party commits a material breach of the Agreement and fails to cure such default to the non-defaulting party’s reasonable satisfaction within thirty (30) days. In the event of termination Customer shall pay Wipro for goods delivered and services rendered till the date of termination.	As per RFP
169	Additional Hardware	Clause not present in RFP	Notwithstanding anything to the contrary in the RFP, any requirement by Purchaser of any additional Hardware under the Agreement shall be provided by the Successful Bidder at an additional cost to Purchaser and the same shall be done through a Change Order.	As per RFP
170	Upgrades/Enhancements	Clause not present in RFP	Notwithstanding anything to the contrary in the RFP, any requirement by Purchaser of any upgrade/enhancement shall be provided by the Successful Bidder at an additional cost to Purchaser and the same shall be done through a Change Order.	As per RFP
171	Penalty Cap	Clause not present in RFP	Nothing withstanding anything contained here, including annexures etc, the maximum aggregate penalty against the bidder for all claims, by which ever name so called, shall be limited to 3% of the respective SOW/PO and shall be in lieu of all available remedies. Also, Wipro does not agree to any form of risk purchase.	As per RFP
172	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 51, Point :4.5	The proposed solution must have built-in hardware bypass for all interface types.	Please clarify, whether the solution should be deployed in standalone mode or in High Availability. If NIC is opting for High Availability, then Bypass solution should not be asked. As Bypass solution can not work with high availabilty. If one appliance failes, traffic will be bypassed and will not shift to other HA applaince.	Solution shoud be deployed in standalone mode

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
173	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 51, Point :4.8	The proposed solution should support Multiple Segment protection minimum of 2X10Gig Segments and 4 X 1 Gig segments with internal bypass mechanism for all segments	Please clairify how many ISPs currently NIC is haiving. The port Density which is asked is quite huge for Enterprise Data Center. Please clarify, whether the solution should be deployed in standalone mode or in High Availability. If NIC is opting for High Availability, then Bypass solution should not be asked. As Bypass solution can not work with high availabilty. If one appliance failes, traffic will be bypassed and will not shift to other HA applaince.	Solution shoud be deployed in standalone mode
174	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 51, Point :4.16	The proposed solution should be able to work in fail open mode in all the ports and should support software bypass capability.	Please clarify, whether the solution should be deployed in standalone mode or in High Availability. If NIC is opting for High Availability, then Bypass solution should not be asked. As Bypass solution can not work with high availabilty. If one appliance failes, traffic will be bypassed and will not shift to other HA applaince.	Solution shoud be deployed in standalone mode
175	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 51, Point :4.19	OEM of the proposed solution should have deployed the DDOS detection and mitigation solution in at at-least 4 ISP's in India, these systems deployed at ISP's should be used for offering DDOS detection and mitigation services to ISP's of NIC. Adequate information/documents should be provided to support the references.	Since the solution is asked for Enterprise Data center, but the OEM eligibility has been asked for Internet Service Providers. Also, Please clarify the ISPs being used in NIC. On premise DDoS Solution is not ISP Dependent. Hence Kindly dilute the clause.	As per RFP
176	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 53, Point :4.39	The proposed solution should Protect against SSL/TLS- encrypted Attacks with a FIPS-2 compliant Internal SSL module	FIPS-2 certification is required to deploy SSL Appliance in United States in Govt Organisations. It has no significance in India. This certification is majorly applied to the OEMs from United states. This is completely defeating the purpose of Make In India Initiative as well. Kindly dilute the clause.	As per RFP
177	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 53, Point :4.43	Device should have at least 4 x 10G bypass Interfaces plus 8 X 1 GE bypass interface with Hot swappable Dual Power supply.	This is favoring to One OEM. IN today's age all the Network ports are SFP+, in which customer hss a liberty of changing the same hardware port to 10G or 1G fiber or 1G Copper. Hence Please change it to 12SFP+ ports.	This is minumum asked. The bidder can quote hardware matching the same more interfaces
178	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 53, Point :4.45	The proposed solution must support CLI access over RS-232 serial console port, SSH.	RS-232 is an older technology . All the new apliances are coming with RJ45 Console Ports. Kindly add RJ45 Console Ports into Serial Console.	It can be RS-232 0r RJ45
179	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 53, Point :4.55	The proposed solution should have scalable inspection throughput license approach from 2 Gbps to 20 Gbps without additional hardware	This specification is favouring to a Single OEM. Being a leader in this technology, we have never seen a scalability option of 10 times. Kindly Ammend it to 2 Gbps scalable to 4 Gbps which is 100% scalability.	RFP Clause amended as follows,"The proposed solution should have scalable inspection throughput license approach from 2 Gbps to 10 Gbps without additional hardware"
180	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 53, Point :4.56	The proposed solution must support at least 15 Million legitimate concurrent sessions and unlimited attack concurrent sessions & must support 2 Million Layer4 connections/second	This clause is limiting our participation. Kindly ammend the legitimate concurrent connection to 10 Million.	As per RFP
181	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 54, Point :4.59	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.	This favouring to one OEM. Kindly change the Flood Attack Prevention rate to 20 MPPS.	The minimum specification is for 15 MPPS. The bidder can quote for higher.

NIC/IT/RFP/NXGThreatProtect/RFP/07/2017
NEW DATE AND TIME OF BID SUBMISSION: 28-03-2018 till 3:00PM
DATE AND TIME OF BID OPENING: 28-03-2018 from 4:00PM

SL.No.	Page Number; Point Number	Clause Description	Query description	Response
182	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 54, Point :4.61	System Should inspect and mitigate encrypted attacks up to - 40k SSL CPS with 1K Key size. - 8K SSL CPS with 2K key size.	This is favouring to One OEM. IN current age scenario the world is communication SSL on ECC cipher and TLS 1.3 . There is no mention of TLS1.3 or ECC in this Tender. Kindly add the ECC parameters to at elast 10k ECC connections per second.	TLS 1.3 & ECC should be supported
183	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 54, Point :4.65	Cloud DDOS Service Provider shall have a purpose-built network of mitigation centers with at least 4Tb of mitigation capability.	This is favouring to one OEM and limiting our partiiaption. Kindly ammend the mitigation capability to 3 Gbps.	As per RFP
184	63.5, Technical Compliance – Next Generation Threat Protection Solution, Page 56, Point :4.98	The proposed solution must support receiving flow telemetry from NIC outers in order to detect DDoS attacks and trigger cloud mitigations. This feature should be supported for future requirement	Flow telemetry used in Internet Service Provider network, wheere network topology is MESS. In Enterprise Data Center, Network topology is complete Symetric . Kindly Dialute the clause and allow us to participate.	Accepted