Pre-Bid queries						
Tender Name: Request for proposal (RFP) for selection of System Integrator for managing On-Site Security Operation Centre (SOC) for Stockholding						
Ref No.	**IT-10/2023-24**					**Date: 23-Feb-2024**
S. No.	**Page No. & Reference Clause**	**Point /Section #**	**Category (Eligibility / Scope / Commercial / Legal / General)**	**Clause Details**	**Query/seeking clarification**	**Response**
1	Page No. 91	RFP Clause No. VIII Other Provision, Point No.3		If the Contractor is a partnership or a consortium, this IP must be signed by all the partners and consortium members. In case of a Company, the IP must be signed by a representative duly authorized by Board resolution.	Please clarify whether a consortium is permitted for this tender. Furthermore, it is requested that the consortium be allowed to participate in the tender, which should benefit the buyer by ensuring the highest quality competition and the best quality-oriented competitive bid response.	Consortium not allowed
2	Page No. 9 of RFP Clause-Eligibility Criteria, Sr. No.2	Eligibility Criteria, Sr. No.2	Eligibility	Should have an annual turnover of at least Rs. 12 Crores per annum for last 03 (three) financial years (2020-21, 2021-22 and 2022-23). It should be of individual company and not of Group of Companies	It is requested that you please kindly consider the turnover of a group of companies as a factor in both qualification and technical marking for evaluation.	No change
3	Page No. 16 of RFP Clause-Technical Bid Evaluation, Sr. No.1	Technical Bid Evaluation	Sr. No.1	Average annual turnover of the bidder during last 03 (three) years i.e. 2020-21, 2021-22, and 2022-23: 16 Crores >= 40 Crores : 10 Marks >40 Crore but <= INR 80 Crore : 12 Marks More than INR 80 crore : 15 Marks	It is requested that you please kindly consider the turnover of a group of companies as a factor in both qualification and technical marking for evaluation.	Consortium not allowed

4	11	Eligibility 12	Eligibility	Bidder to provide undertaking that no penalties, amounting to up to 5% of the contract value per year, have been imposed in the last 03 (three) years by any of its client(s).	Need clarity on this point	Self-declaration by bidder from authorised signatory that no penalty has being imposed by any of its clients in the last 3(three) years as a part of service agreement.
5	9	Eligibility 1	Eligibility	The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of managing SOC services and Network-Security device management for the period of 7 years before RFP date. Copy of Certificate of Incorporation issued by the Registrar of Companies and Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory along with supporting documents for SOC related PO.	We are company registered under companies act 1956 so in this case do we have to provide both Certificate of Incorporation & Self declaration for SOC related PO	Yes
6	35	APPLICATION PENETRATION TESTING-GRAY BOX	Scope	What is the total number of applications in scope?		20
7	35	APPLICATION PENETRATION TESTING-GRAY BOX	Scope	Kindly share the application bifurcation of the inscope items (Mobile/web/thick client)		Will be provided to Successful bidder from total 20 Applications.
8	33	Vulnerability Scanning	Scope	Is vulnerability management program required or one time scans are in scope?		Vulnerability management program is required
9	33	Vulnerability Scanning	Scope	Is vulnerability remediation also in scope (followup for closure)		YES
10	33	Vulnerability Scanning	Scope	Is there any existing VA tool or Inspira is supposed to bring own tool?		Bidder should bring their own on premise tool for VA/PT and Configuration audit

11	19	Understanding of Scope - Endpoint Security		Currently StockHolding has on-premise Endpoint detection and response (EDR) solution from TrendMicro. During the future course of action StockHolding may use cloud based XDR Solution	Is bidder expected to procure a new cloud based XDR solution or Stockholding will procure by themselves	No, Bidder has to manage and support be it on premise or cloud based EDR / XDR.
12	24	Understanding of Scope - SOC Operations		System Integrator will establish full featured cloud based Managed Detection and Response (MDR) Services along with Incident Management capabilities	Should propose their own SOC services or Stockholding will procure from different partner & bidder is just expected to manage them.	Bidder should propose, procure, provide and manage full featured SIEM /MDR services (till new MDR services are fully implemened and integrated bidder should support existing MDR by co ordinating and closure of tickets)
13	28	Managed Detection and Response services		Auto Containment: MSSP's auto remediation to quickly contain threats by enabling rules on firewall, NGFW, IPS, Proxy, EDR, WAF, Patch management, Routers or AD. MSSP will integrate our security devices and push rules based on pre-defined response playbooks, for us	Does Stockholding also want bidder to propose their SOAR services?	SIEM/MDR solution should be capable of providing SOAR features
14	54	MDR Sizing		The expected EPS count for StockHolding should be a minimum of 2,000 and scalable to 5,000. The System Integrator needs to coordinate with MDR team and provide support for MDR services that cater to as per the requirement of devices on boarded with MDR.	Does Stockholding already have MDR services in place with another team and wats the bidder to just manage them?	Bidder should propose, procure, provide and manage full featured SIEM /MDR services (till new MDR services are fully implemened and integrated bidder should support existing MDR by co ordinating with support vendor and closure of tickets)
15	NA	NA	General query		Does Stockholding want bidder to provide premium or free threat intel feeds services?	Premium but not exclusive to us, Threat intel feed of bidder SOC can be shared with Stockholding

16	NA	NA	General query		What solutions for MDR is stockholding currently using?	Aissac
17	NA	NA	General query		What solutions for SIEM is stockholding currently using?	Aissac
18	NA	NA	General query		Apart from 11 onsite resources, the other resources can operate from Bidder SOC. Please confirm if this understanding is correct	No resource except SOC, which means All device management resources should be on premise
19	61	SLA Penalty	SLA Penalty	The maximum penalty applicable will be 10% of the monthly billing.	We request to modify it as conditions - The maximum penalty applicable will be 5% of the monthly billing.	Not accepted
20			General query	Delivery Timeline		-
21	82	Eligibility Criteria (For On-site Manpower Assignment) – Total 11 nos. (B)	`	Last 3 Months Payslips / Appointment letter of present organization Resume of the resources proposed	Request to remove this clause.	No change
22	45	Proposed Team - Sl. 3 - Security Consultants (6)		in this clause the security consutant for 24x7 is mentioned 6Nos.	request to increase the resource count to 9	It is up to Bidder to factor to manage resources but at any given day 11 resources must be on site and all factored resources should be dedciated to Stockholding project only.
23	NA	NA		General query	request to clarify - onsite resources are responsible for only device management tasks mentioned under A. Device Management of page No. 51 rest all other tasks like log monitoring, MDR/SIEM monitoring will be done in Bidders SOC.	on site resources who are responsible for Device management team also responsible for co odinating with SIEM-MDR service provider and manage tickets till closure of the same
24	NA	NA		General query	Which OEM for DLP ?	Currently IDLP is in use, Stockholding planing to go with full fledge DLP (Endpoint , Web and Email) in future
25	NA	NA		General query	What are the number of endpoints ?	2500 to 3000

26	NA	NA		General query	What are the number of current Incidents per day/month for DLP	per day around 400 might change when full fledge DLP is in place.
27	NA	NA		General query	The DLP covers Endpoint and Email (only). Please confirm	As of now email and end point
28	24	NA		General query	In future System Integrator will configure and integrate Database Activity Monitoring (DAM),	Yes
29				General query	Is Security testing and consulting outside of the 11 member team's scope, which needs to be factored as a separate line item ?	Yes
30				General query	Please let us know the total number of servers for Business envornment and IT envionrment	160
31				General query	Please share the type and number of applications	20
32				General query	Pls share the total number of users and end points	2500-3000
33				General query	Please share the appx policies appliable in each Firewall	300
34				General query	How many VPN tunnels are there in each Firewall?	25, same will increase once SDWAN is implemented
35				General query	Please share the count of VPN users are there in each in each region	total users 600
36				General query	How many applications are published on the internet?	10
37				General query	How many applications are on boarded to WAF	16
38				General query	How many applications are integrated with Loadbalancer	8
39				General query	Please share the noumber of links per site and also the type of links like whether MPLS or internet.	ILL -6

40	9	ELIGIBILITY CRITERIA (Documents to be Submitted Online)		The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of managing SOC services and NetworkSecurity device management for the period of 7 years before RFP date	Request Stock holding to consider below clause for competitive bid participation - The bidder should be a company registered under Indian Companies Act, 1956 or a Partnership Firm registered under Indian Partnership Act, 1932 with experience of managing SOC services and Network Security device management for the period of **5 years** before RFP date	No change

41	9	ELIGIBILITY CRITERIA (Documents to be Submitted Online)		The bidder should have executed or managed from customer premise, during last 05 (five) years with any one of the following: 01 (one) SOC contract with networksecurity device management from customer premises having value not less than INR 2.4 Crores for any Corporate entity in India OR • 02 (two) SOC contract with networksecurity device management from customer premises having value not less than INR 1.5 Crores each for any Corporate entity in India OR • Three SOC contract with networksecurity device management from customer premises having value not less than INR 1.2 Crores each for any Corporate entity in India	As the Bid Estimate is more than 6 crore, we request stock holding to consider work experience at least 50% of the bid estimate as below: The bidder should have executed or managed from customer premise, during last 05 (five) years with any one of the following: • 01 (one) SOC contract with networksecurity device management from customer premises having value not less than INR 3.4 Crores for any Corporate entity in India OR • 02 (two) SOC contract with networksecurity device management from customer premises having value not less than INR 2.0 Crores each for any Corporate entity in India OR • Three SOC contract with networksecurity device management from customer premises having value not less than INR 1.6 Crores each for any Corporate entity in India	No change
42	9	ELIGIBILITY CRITERIA (Documents to be Submitted Online)		SIEM solution provided by bidder shall be in Gartner/Forrester Leaders Quadrant since last 03 (three) years viz. 2021, 2022 & 2023	Request Stock holding to consider below clause for OEM participation SIEM solution provided by bidder shall be in Gartner/Forrester Leaders Quadrant **in any of** last 03 (three) years viz. 2021, 2022 & 2023	No change

43	12	ELIGIBILITY CRITERIA (Documents to be Submitted Online)		(B) Criteria Proposed resources must be on the Payroll of bidder (out-sourcing staff not allowed) Documents to be submitted by successful bidder Last 3 Months Payslips / Appointment letter of present organization Resume of the resources proposed	Request to consider self declaration to be provided by bidder for as per RFP. As the resource deployment shall be place on award of contract subject to approval from stockholding. (B) Criteria Proposed resources must be on the Payroll of bidder (out-sourcing staff not allowed) Self declaration documents to be submitted by successful bidder	No change
44	14	Technical Bid Evaluation		The number of professional staff in the area of Information Security (CISA/CISM/CISSP/CEH/ISO 27001 certified) certified person on bidder Payroll. Atleast 15 nos. Certified person – 7 Marks 15-40 Certified persons – 10 Marks More than 41 Certified persons – 15 Marks	As the requisite no will give particular advantage, Hence we request you to consider below clause inline to the requirement. The number of professional staff in the area of Information Security (CISA/CISM/CISSP/CEH/ISO27001 certified) certified person on bidder Payroll. Atleast 15 nos. Certified person – 7 Marks 15-40 Certified persons – 10 Marks More than 30 Certified persons – 15 Marks	No change
45	22	h) Active Directory Management (Standalone as well as on Private cloud deployment)		• Migration active directory from 2016 to 2019 & from 2019 to 2022 • Server integrate in domain and reboot,Migration of SOC servers in Domain.	Does the stock holding wants Ad Migration Implementation Professional. We request Stockholding resource scope to Operational Management to bring the expertise out of here.	Yes, bidder should provide expertise support from backend if required for AD migration implementation.

46	23	k) Support for Secure Network Virtualisation NSX-T with VMware for StockHolding's private Cloud		NSX integration with SIEM-MDR platform and creation of use cases as per the requirements	Please share usecase and integration expectation.	Industry best use cases for BFSI has to be integrated for each device is required and this might change time to time.
47	24	B. SOC Operations		The System Integrator will develop the work flow process for attending to the various functions at the SOC including the work flow for attending to the incidents generated with network-security device management.	Request Stockholding to confirm existing ITSM for bi-directional integration and ticket workflow Management	Stockholding is in process of procuring ITSM tool. As of now it is manual
48	28	• Threat Hunting:		• Threat Hunting:	Please confirm frequency for threat hunting	Expected to be done automatically where as manual actrivity can be done month once
49	29	D. Security Testing Network Penetration Testing Configuration Audit (CA), Vulnerability Assessments (VA) & Penetration Testing (PT) - (As per CIS Benchmark and close the gap's and provide the clean report)		D. Security Testing Network Penetration Testing Configuration Audit (CA), Vulnerability Assessments (VA) & Penetration Testing (PT) - (As per CIS Benchmark and close the gap's and provide the clean report)	Does the bidder utilize the existing Tenable VM solution for Vulnerablity Management for security testing. Please confirm.	Bidder should bring their own on premise tool for VA/PT and Configuration audit
50	54	MDR Sizing		MDR Sizing The expected EPS count for StockHolding should be a minimum of 2,000 and scalable to 5,000.	As EPS count is uncertain and may increase during the contract period, Hence to ensure request you to confirm no. of device.	300 devices

51	54	Logging of critical devices		Logging of critical devices • The System Integrator is required to maintain the syslog of critical network devices installed at DC, DRC and Critical locations for a period of three months. The logs should be onsite for three months thereafter logs can be stored on tapes and submitted to StockHolding.	As per CERT-IN, our recommendation is for 180 Online and 180 Offline. Request for log retention as per CERT-IN for MDR Service. After Log retention period, these can be export or archive over tape/storage of Stock Holding. Hence, bidder must provide flexiblity to export or transfer these logs through secure channel.	Yes
52	56	Development of Connectors for customized applications/ devices.		Development of Connectors for customized applications/ devices. While it is expected that connectors for all the standard applications and devices will be readily available in the collector and Log management devices, connector for mostly in-house/custom built applications will need to be developed. As MDR team deployed for SOC operations will be expected to develop applications connector, in house SOC team of System Integrator expected to support them for integration of devices as per the custom connectors provided to them by MDR team	How many custom parser are required for MDR integration. Please confirm no of custom application or non standard device for efforts consideration	It depends on proposed solutions Api support . Minimum 10 custom parsers might needed per year.

53	56	D. Security Intelligence Services		D. Security Intelligence Services	Please confirm no of External Threat Intelligence must be ingested into the MDR service for faster detection and response. Multiple threat inteligence service provides better enrichment and it enhances threat detection capability and eliminates the dependency of native SIEM threat intel bring the mature/diverse geographic intel feeds/IOC staying ahead of time.	Bidders SOC should have multiple premium threat inteligence feeds integrated with SIEM / MDR services to provide the same to Stockholding as part of SOC services
54	65	Root Cause % of RCA report submitted (Critical) Total number of RCAs submitted within 48Hrs./ Total number of RCAs		Root Cause % of RCA report submitted (Critical) Total number of RCAs submitted within 48Hrs./ Total number of RCAs	Request Stockholding to consider 72 hrs for RCA submission.	Not accepted
55	67	G. Managed Detection and Response and Other Services: 24x7x365 days Security Log Monitoring Services of in scope Devices management and Arc sight (SIEM service)		G. Managed Detection and Response and Other Services: 24x7x365 days Security Log Monitoring Services of in scope Devices management and Arc sight (SIEM service)	Does the scope also include monitoring of ArcSight SIEM Service. Please confirm on understanding here.	Existing SIEM /MDR will be active till newly proposed SIEM/MDR services are full implemented and integrated.
56	3	Last Date for Submission of Online Bid -27-02-2024 15:00:00			Request for bid extension till 7th March 2024 as scope of SOC is service oriented and should comply with eligibility criteria, technical specification, resources and scope of work	Bid Extension provided till 05-Mar-2024 15:00 Hrs

<table>
<tr>
<td>57</td>
<td></td>
<td></td>
<td></td>
<td>Pls refer page 69 H section for MDR SLA</td>
<td>Proposed SLAs for MDR are as follows:
<table>
<tr><th rowspan="2">Critical Service Level Category</th><th colspan="2">Measures</th><th rowspan="2">Remarks</th></tr>
<tr><th>Response Time</th><th>Expected Service Level</th></tr>
<tr><td>Service outage notification (P1)</td><td>30 Mins</td><td>99.00%</td><td>P1 – Successful Attack, compromise, Virus outbreak etc.</td></tr>
<tr><td>Severity 1: Incident detection case creation</td><td>30 Mins</td><td>98.00%</td><td>P2 – High Priority Alert from integrated devices, Policy Violations, multiple scans.</td></tr>
<tr><td>Severity 1: Incident remediation case update</td><td>45 Mins</td><td>98.00%</td><td>P3-Low Priority Alerts from integrated devices, limited scan, recon, infections etc.</td></tr>
<tr><td>Severity 2: Incident detection case creation</td><td>2 Hour.</td><td>97.00%</td><td></td></tr>
<tr><td>Severity 2: Incident remediation case update</td><td>4 hours</td><td>97.00%</td><td></td></tr>
<tr><td>Severity 3: Incident detection case creation</td><td>4 hours</td><td>96.00%</td><td></td></tr>
<tr><td>Severity 3: Incident remediation case update</td><td>8 hours</td><td>96.00%</td><td></td></tr>
</table></td>
<td>No change</td>
</tr>
<tr>
<td>58</td>
<td></td>
<td></td>
<td></td>
<td>Pls refer page 76 for termination clause</td>
<td>Either of the party reserves right to terminate the contract by giving 30 days prior written notice in advance</td>
<td>Your understanding is correct.</td>
</tr>
<tr>
<td>59</td>
<td></td>
<td></td>
<td></td>
<td>One-time Implementation Cost– 100% payment after successful completion</td>
<td>One-time Implementation Cost– 50% payment on kick off; 50% payment on implementation and sign off</td>
<td>No change</td>
</tr>
<tr>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td>Pls check the penalty clause in page 62</td>
<td>Need discussion as the same is not acceptable by our Legal and Finance</td>
<td>Penalty clause will be as per RFP terms and consitions</td>
</tr>
<tr>
<td>63</td>
<td></td>
<td></td>
<td></td>
<td>Resources Management penalties (page 63,64)</td>
<td>Not approved by our Legal and hence need discussion</td>
<td>No change</td>
</tr>
</table>

64				Any dispute or difference arising between the parties with regard to the terms of this Agreement / Pact, any action taken by the Principal / Owner / StockHolding in accordance with this Agreement / Pact or interpretation thereof shall not be subject to arbitration.	Not approved by our Legal and hence need discussion	No change
Note: All other clauses/Terms & conditions except above shall remain same as per RFP (RFP Reference Number: IT-10/2023-24)						