CORRIGENDUM / AMENDMENT-2 TO Managed Security Services for Security Operation Centre

CORRIGENDUM / AMENDMENT-2

With reference to the query received from vendors (bidders), following are the amendments to the RFP Reference No. IT-03/2017-18 dated 13/07/2017

I. **Eligibility Criteria** (Amendments dated 8th August 2017)

SN.	Old Criteria	Replaced with new Criteria
5	The vendor (bidder) should have minimum Rs. 50 Crore turnover and should be profitable in last two years	The vendor (bidder) should have minimum Rs. 50 Crore turnover.
7	Bidders should have at least 10 certified personnel with specific certifications such as CISM, CISSP, GCEH, CISA, SIEM etc.	Bidders should have adequate certified personnel with specific certifications such as CISM, CISSP, GCEH, CISA, SIEM etc.
8	Bidder should be recognized by independent agency like Gartner for its capability for Managed Security Services	This clause is Removed

Limitation of Liability: Will be limited to the extent of a maximum of the total cost of PO value.

II . **TECHNICAL ELIGIBILITY**

The Technical eligibility Criteria is modified as below. (The Technical eligibility criteria mentioned in page 7 to 10 in the RFP is replaced with the below mentioned technical eligibility criteria). The total Maximum marks are changed from 300 to 400 marks.

S.No	Description	Certification	Documents	Maximum Marks

1	The Bidder should have minimum 3 years of experience in providing Network Security device management such as installation, configuration & management of network-security devices (Firewall, IPS Appliances, Proxy Services, Antivirus / Antimalware support services, ACS Applainces, Load balancers, Spam mail Services) L3 & L2 network devices out of which at least 3 years of experience in a Scheduled Commercial Bank/Central Government of India Organization having at least 1000 branches in India. Mandatory Compliance: >=3 Scheduled Commercial Bank/Central Government of India Organization having onsite SOC Implementations and Operations Assignments (25 Marks)	NA	Self-declaration on bidders letter head, confirming the mentioned criteria.	25
2	The Bidder should own and have been managing a well established full featured SIEM solution, Security Operations Centre (SOC) in India, and should have minimum 5 years of experience in delivery of a full featured end-end hybrid SIEM system as a service, out of which at least 3 year of experience in a Scheduled Commercial Bank/Central Government of India organization having at least 1000 branches in India. Mandatory Compliance: >=3 Scheduled Commercial Bank/Central	NA	Self-declaration on bidders letter head, confirming the mentioned criteria.	25
3	Bidder should be recognized by independent agency like Gartner for its capability for Managed Security Services and Bidder should be CERT IN Empaneled member Mandatory Compliance: 25 Marks.	NA	Self-declaration on bidders letter head, confirming the mentioned criteria.	25
	Non-Compliance:			

4	The bidder's should have a reference of managing and monitoring security operations centres (SOC) of at least one large customer similar to any PSU Indian Bank for a minimum period of 3 years. Such reference client network must have No.of network-security devices (Excluding L2 and L3 Switches etc.) Less than 50 devices, then 05 Marks 50-100 devices, then 15 Marks 100+ devices, then 25 Marks	NA	Customer signoff/	25
5	Number of years of experience in the field of Security management of PSU banks in India. No of Years : 1 year - 3 years, then 5 marks More than 3 years to 5 years, then 15 Marks More than 6 years to 10 years, then 25 Marks.	NA	Customer signoff/	25
6	No of Trained and Certified Employees with valid certifications, having 1 year relevant experience (post certification) is with the bidder, and who would be made available for deployment onsite. No. of CISSPs / CISMs: if >10, then 25 Marks if <10 & >05, then 15 Marks	CISSP / CISM	Self-declaration on bidders letter head, confirming each of the mentioned criteria.	25
7	If <05, then 0 (Zero Marks)No of Trained and Certified Employees with valid certifications, having 2 years relevant experience (post certification), out of which 1 year experience is with the bidder and who would be made available for deployment onsite, as per the RFP. No. of CCSEs:	CCSE	Self-declaration on bidders letter head, confirming each of the mentioned criteria.	25

	if >25, then 25 Marks if <25 & >15, then 15 Marks If <15 & >05, then 05 Marks			
8	No of Trained and Certified Employees with valid certifications, having 2 years relevant experience (post certification), out of which 1 year experience is with the bidder, and whose service's the bidder would make available to the Corporation, onsite, in case of security related emergencies/ severe outages/troubleshooting/design and implementation as may be required in the course of the delivery of services by the bidder. No. of CEHs: if >25, then 25 Marks	CEH	Self-declaration on bidders letter head, confirming each of the mentioned criteria.	25
9	No of Trained and Certified Employees with valid certifications, having 2 years relevant experience (post certification), out of which 1 year experience is with the bidder, and whose service's the bidder would make available to the Corporation onsite, in case of SIEM tools related emergencies/ severe outages/troubleshooting/design and implementation as may be required in the course of the delivery of services by the bidder. if >10, then 25 Marks	SIEM Solution	Self-declaration on bidders letter head, confirming each of the mentioned criteria.	25

if <10 & >5, then 15 Marks

10	No of Trained and Certified Employees with valid certifications, having 5 years relevant experience (post certification), out of which 3 year experience is with the bidder, and whose service's the bidder would make available to the Corporation, onsite, in case of defining and implementing ITIL service lifecycle as	ITSM	Self-declaration on bidders letter head, confirming each of the mentioned criteria.	25

	may be required in the course of the delivery of services by the bidder. if >5, then 25 Marks			
11	No of Trained and Certified Employees with valid certifications, having 5 years relevant experience (post certification), out of which 3 year experience is with the bidder, and whose service's the bidder would make available to the Corporation, onsite, in the course of implementing and delivery of the services by the bidder. if >10, then 25 Marks	PMP	Self-declaration on bidders letter head, confirming each of the mentioned criteria.	25
12	Presentation on the Offered Network-Security device management Service should include:- • Network-security devices management and SIEM tool as a service management. • Methodology adopted for Incident, Change and problem management. • Vendor Co-ordination. • SLA tracking and escalation managements.	NA	Presentations by B	25
13	The Bidder should be included in either Gartner or Forrester Report for Managed Detection and Response. Yes - 15M No- 0M	NA	Self-declaration on bidders letter head, confirming the mentioned criteria.	15
14	The Bidder should to do threat hunting using security analytics models, instead of only use case, rules and signature based detection. Proof to be submitted for each capability. Use Cases – 5 Points Rules and Signatures – 5 Points Security Analytics Models – 5 Points	NA	Self-declaration on bidders letter head, confirming the mentioned criteria.	15

15	The bidder should be able to Monitor alerts from SIEM, Triage alerts from SIEM, IPS, WAF etc., Fetch logs in real time for investigation, automate remediation using on premise platform. Alert Monitoring – 5 Points Triage - 5 Points Fetch logs in real time – 5 Points Automate Remediation Process – 5 Points	NA	Self-declaration on bidders letter head, confirming the mentioned criteria.	20
16	Following roles are expected from bidder's SOC Security Analyst – 5 Points Incident Handlers – 5 Points Threat Hunters ---Malware, Network, endpoint, and phishing etc. related threats in North-South and East-West traffic of SCHIL. - 5 points Data Scientists --- Big Data Scientists to build security models to detect anomalies using industry best algorithms. – 5 Points Malware Engineers – Detect Patient Zero, Attack origin and blast radius as part of RCA of confirmed incident. – 5 Points	NA	Self-declaration on bidders letter head, confirming the mentioned criteria.	25
17	Centralized Dashboard to Management Top Alerts/Risks – 5 points Drill Down Graphs – 5 Points Risk Posture and Maturity Level – 5 Points Graphical display of application security status based on locations, business units – 5 Points Heat Map view of each Business Unit to understand the risk exposure of each BU (Capture risks in each asset) – 5 Points	NA	Self-declaration on bidders letter head, confirming the mentioned criteria.	25
	Total			400

The below points are amended in the RFP on 8th August 2017. These points are in addition to the scope mentioned in the RFP (refer Page No 13 onwards in the RFP documents)

Additional Points :

Detailed Scope of Work

- SLA Management.
- Network security devices Incident, change and problem management.

- The bidder has to manage, maintain, configure, add, remove, modify, log calls for repair, update and upgrade all installed in-scope network-security equipment's, at DC, DR, Extranet DR, etc.
- The bidder will evaluate, troubleshoot, reconfigure and rectify system performance under normal and degraded conditions and perform periodic fine tuning to ensure maximum network availability.
- The bidder has to perform warranty, inventory, AMC & Vendor Management to enable coordination with internal & external agencies including Internet SPs for replacement or relocation of any hardware/software/service components.
- The bidder will perform Internet Services Management, Vendor Management, Asset Movement and Management.
- The bidder will supply the necessary expertise and templates to implement the service delivery processes and procedures as per ITIL/ITSM/ISO 27001:2013/Basel II guidelines / framework, required for the smooth functioning of the said managed services, from time to time during the period of this contract.
- The bidder will ensure 24X7x365 network-security device management and SIEM service availability through onsite and remote network-security devices monitoring and management through SIEM tool. It will be the responsibility of the bidder to take immediate actions to ensure 24x7x365 network-secuirty services availability.
- The bidder will ensure the deployed resources for network-security device management will look into the end to end business application availability, reachability and user experience from the network-security perspective.
- The bidder will ensure to maintain a comprehensive professional documentation of the network-

security device management under this contract.

- The bidder will ensure regular comprehensive reporting on health of in-scope Network-security devices, equipment's under DC and DR.

Security Information and Event Management (SIEM) Services with ArcSight :

- Proposed ArcSight Solution should have physical segregation of roles of Collector, Log Management and Correlation layer with some enhanced features of Log Management layer. Log Management solution should have separate UI for searching, reporting, basic dashboards etc even if Correlation layer is down or not available. i.e. Logs should be available for audit even if correlation is down.

- Bidder should propose ArcSight Data Platform which includes Loggers, Connectors, ArcSight Management Center, Customer parser Development and Event Broker. Solution should support forwarding of logs (raw or normalized) to any third party solution or to any big data platform like Hadoop with the help of event broker if stock holding plans to deploy it in future.

- Three Months online and 3 months archival should be proposed. Archival should be readable. Post that all the logs should be stored on Tapes. Total of 7 year of logs should be maintained.

- Collectors should be in HA in DC & DR. Log management & Correlation layer should be in standalone at each location.

SERVICE LEVEL AGREEMENT AND PENALTY:

SOC Operations :

Serial Number	Service Area	Criticality	Service Level
3	Security Intelligence Services and Reports.	Important	Advisories within 24 hours of new global threats & vulnerabilities disclosures.

Monitoring and management of Network-Security devices:

Event	Criticality	Timeframe		Penalty Calculation	Compliance (Monthly / Quarterly)
Urgent configuration changes required to maintain normal business operations	High	Response Time : 15 min	Resolution time: 60 min	For each instance of breach, penalty will be INR 5,000	Monthly 100%

Create, modify and delete configurations in network-security devices after obtaining approval from Stockholding Team.	Medium	Response Time : 15 min	Resolution time: 2 hour	For each instance of breach, penalty will be INR 5,000	Monthly 100%
Review of capacity planning of in-scope network-security devices. Details of under utilized and over utilized network-security devices. Recommend plan to procure/upgrade/optimize/mitigate the over utilized Network-security devices.	Medium	Response: Starting on the 1st day of the first month of the start of every Quarter.	Resolution: Within 5th day of the first month of the start of every Quarter.	For every 1 week of delay or part thereof, the penalty will be INR 5,000	Quarterly 100%
Asset Inventory : Loss of any network-security assets, under the control of the onsite team, due to omission or negligence or failure, to follow the due process in asset handling (change, movement etc) and thereby updating the network inventory.	High	Response Time : Immediate (as and when asset change/movement occurs)	Resolution Time : Immediate (as and when asset change/movement is completed with appropriate checks)	For each instance of breach, penalty will be INR 5,000, in addition, the purchase value of the lost asset at that period of time will be recovered.	Monthly 100%
Reports and MIS	High	Daily : Before 10:00AM Weekly : Before 10:00AM Monthly : By 7th of every month		For each instance of breach, penalty will be INR 5,000.	Monthly 100%

Incident Management, Vendor Management and Investigation

Event	Criticality	Timeframe		Penalty Calculation	Compliance
Availability of Network Devices.	High	Response time: (A) Immediate during the 16 hour window (7 AM to 11 PM X 6 X 365) via (onsite) proactive monitoring using extended functionality of remote SOC services of the bidder.	Resolution Time : (A) 1 hour (B) 2 hour	For each 0.1% or part there of drop in SLA, penalty will be INR 25,000	Monthly 100%

		(B) 2 hours (11 PM to 7 AM X 7 X 365) on all other week days, Sundays and any other Public Holidays) from the time the call is logged by the Stockholding Team.			
Call/Ticket logging with network-security devices / link Support and managing vendors.	High	Response time-15 min	Resolution Time : As per the agreed SLA between external vendor and Stockholdin g	For each instance of breach, penalty will be INR 5,000	Monthly 100%
Call/Ticket logging to OEM/SI/Vendor for device malfunctioning (call should not be rejected by OEM/SI/Vendor citing configuration issue)	High	Response time-15 min	Within vendor SLA	For each instance of breach, penalty will be INR 5,000	Monthly 100%
Ensure call logged to OEM/SI/Vendor/Link Provider are resolved within their signed SLA with OEM/SI/Vendor/Servic e Provider.	Medium	Within vendor SLA		For each instance of breach, penalty shall be INR 2,000. FMS to ensure that calls are constantly followed-up & closed. If required, should be escalated to Stockholding network team promptly as per escalation matrix for immediate action.	Monthly 100%
Incident reporting	High Medium Low	Response-Immediate Response- 15 minutes. Response-30 minutes.	Resolution-Within 1 hours. Resolution-with in 2 hours Resolution-Before next day 8 AM		Monthly 100%
Reporting of License/AMC/ATS expiry of in scope	High	Response time-90 day prior to expiry		For each instance of breach, penalty will be INR 5,000	Quarterly 100%

devices to SHCIL team for renewal.					

Resource Management :

Event	Criticality	Timeframe		Penalty Calculation	Penalty Calculation
Unavailability of resource on site.	High	Response Time : Immediate	Resolution Time: Immediate	For each instance of breach, penalty will be INR 5,000	Monthly 100%
Late Coming/Early departures will be considered as absent for the day.	High	Response Time : Immediate	Resolution Time: Immediate	For each instance of breach/resource, penalty will be INR 5,000	Monthly 100%
The full resource strenght as agreed in the PO should be depolyed onsite per day per month for the entire contract period.	High	Response Time : Immediate	Resolution Time: Immediate	For each instance of breach/resource, penalty will be INR 5,000	Monthly 100%
Additional certified skilled resource/s having greater expertise/skillsets/knowledge than the incumbent onsite team should be deployed, to supplement the efforts of the on-site support team during emergencies and contingencies (ie for incidents/events bearing severe impact on systems under scope)	High	Response Time : Immediate	Resolution Time: Immediate	For each instance of breach, penalty will be INR 5,000/hour till resolution is made, capped at Rs 50000/-	Monthly 100%
Any/All, trainings aligned for the onsite resources of the service provider, should be intimated by the SP backend team (program manager or equivalent and above) in advance of at least 2 weeks in writing for approvals from the Stockholding team, along with the necessary	High	Response Time : Immediate	Resolution Time: Immediate	For each instance of breach/resource, penalty will be INR 5,000	Monthly 100%

provisioning plan for a shadow/backup resource -inline with the PO OR having greater expertise/knowledge/skill sets and qualification- to be deployed onsite in the event of the original resources being not available for the said training period.					
Seperation of duties (ie use of email ids and login ids across roles)	Medium	Response Time : Immediate	Resolution Time: Immediate	For each instance of breach/resource, penalty will be INR 1,000	Monthly 100%

Monitoring and Management SIEM Tool and Transition Management :

Event	Criticality	Timeframe		Penalty Calculation	Compliance (Monthly /Quarterly)
Proper functioning, Monitoring & Reporting of EMS Tool	High	Response Time : Immediate	Resolution time: 2 hour	For each instance of breach, penalty will be INR 5,000	Monthly 100%
The SP should perform due diligence and submit the reports to StockHolding team have a documented SOC (process, procedure, standard operating procedures (SOP) and MIS etc) inline with the standards followed by SHCIL, and customized to SHCIL environment before starting the SOC operations. These processess, procedures and SOP documents are to be considered as standing documents and hence should be reviewed and updated regularly.	High	Response time: immediate (Time of Service Initiation ie Transition)	Resolution time: At the initiation of formal service after completion of transition process.	For each instance of breach, penalty will be INR 15,000, till resolution is made, capped at INR 150,000.	Transition period completion phase. 100%
The SP should share the complete documentation templates (process,	High	Response time: immediate	Resolution time: At the initiation of	Non-compliance will attract a penalty of INR 15,000/day till	(Before initiation of SOC

procedure, standard operating procedures (SOP) and MIS etc) inline with the standards followed at Stock holding, with the Stock holding team, for approvals, before initiating the SOC services.		(Time of Service Initiation)	formal service after completion of transition process.	resolution is made, capped at INR 300,000.	operations) 100%

Note**:** All other terms and conditions, clauses, annexures and details will be as per RFP Reference No. IT-03/2017-18 dated 13/07/2017 for **Managed Security Services for Security Operation Centre**