Request for proposal for engaging a Managed Security Services provider for SOC for the period of 3 years

Final pre-bid response - post meeting held on 4th Aug -2025

Sr. No.	Document Reference	Page No	Clause No	Description in RFP	Clarification Sought	Additional Remarks (if any)	NPCI Clarification
1	Section 3.1 A - SOC Monitoring	12	3.1.A	Bidder should monitor security logs to detect malicious or abnormal events and raise alerts for any suspicious events.	What is the expected number of log sources (devices, platforms, applications) to be monitored by the SOC team?		40 different Logs sources
2	Section 3.1 A - SOC Monitoring	12	3.1.A	Monitoring should be done on 24/7 basis with onsite personnel/resources.	Is a hybrid operations model (onsite + offsite) acceptable for specific shifts or roles?		Only Onsite
3	Section 3.1 A - SOC Monitoring	12	3.1.A	Bidder should be able to monitor and analyze both internal and external attacks, including databases, applications, and anomalies.	Can you confirm the current list of business applications and infrastructure components to be covered under threat monitoring?		40 different Logs sources, Actual asset details with qulified bidder
4	Section 3.1 A - SOC Monitoring	13	3.1.A	Evidence for any security incident should be maintained in tamper-proof manner and should be made available for legal and regulatory purposes.	Does NPCI already have a tamper-proof evidence management system in place, or should the bidder propose one?		Yes NPCI have tamper proof evidance management system
5	Section 3.1 A - SOC Monitoring	13	3.1.A	Bidder should add/delete/modify rules, reports, and dashboards on SIEM based on NPCI requirements. Quarterly review and optimization is mandated.	Can you confirm the current frequency of SIEM rule modifications and the process for quarterly reviews?		It depends on the evolving threat landscape
6	Section 3.1 A - SOC Monitoring	13	3.1.A	Bidder should provide MIS reports to NPCI on daily, weekly, and monthly basis. Additional metrics such as detection latency, false positive rate, and SOC coverage score should be included.	Please clarify the exact formats expected for daily, weekly, and monthly MIS reports. Are report templates predefined or to be designed by the bidder?		Basis on the compliance requirement MIS report should be modified
7	Section 3.1 A - SOC Monitoring	14	3.1.A	All daily routine and standard activities of L1 and L2 to be fully automated in phased manner within one year.	Can you specify which activities or workflows are to be prioritized for automation in the first phase?		This will be discuss with qulified bidder
8	Section 3.1 B - Incident Response	15	3.1.B	The bidder must perform incident response and containment actions in collaboration with internal teams. An escalation matrix with defined SLAs must be followed.	Please provide the existing escalation matrix and SLAs for critical, high, and medium severity incidents.		This will be discuss with qulified bidder
9	Section - Resource Requirements	16	Resource Requirements	Deployed resources shall create SaaS-based alarm on GCP/AWS.	What is the current cloud environment split across AWS, GCP, or others? Are there containerized workloads requiring log correlation?		Creation of Cloud base alram is optional. But conternerized corelation workloads required from bidder side.
10	Section - Other Requirements	17	Other Requirements	Bidder should prepare the SOC operations for compliance and certification to the standards of ISO 27001, ISO 20000, BS 25999 and PCI DSS.	Are there specific certification gaps NPCI expects the bidder to close within the term of engagement?		All audit/process observation pertaning to ISO 27001, ISO 20000, BS 25999 and PCI DSS manage by bidder
11	Section 3.1 A - SOC Monitoring	13	3.1.A	The bidder should ensure less than 5% false positive rate and work towards minimizing it through continuous improvement.	What is the baseline false positive rate currently observed?		This will be discuss with qulified bidder
12	Section 3.1 A - SOC Monitoring	14	3.1.A	Use cases should be mapped to MITRE ATT&CK framework and updated with emerging threat scenarios.	Is there an existing mapping available, or should the bidder start from scratch?		Existing mapping is available with MITRE ATT&CK framework
13	Section 3.1 A - SOC Monitoring	14	3.1.A	All L1 and L2 tasks are to be automated in a phased manner.	Will NPCI provide a roadmap for phases, or is bidder expected to propose one?		IT will be mutual discussion with qulified bidder
14	Section 3.1 A - SOC Monitoring	14	3.1.A	Rule creation and tuning to be done based on threat intelligence and contextual alerts.	Will NPCI provide internal threat intel sources or expect bidder to onboard feeds?		NPCI will provide
15	Section 3.1 A - SOC Monitoring	14	3.1.A	SOC should detect and respond to lateral movement, data exfiltration, and privilege misuse.	Is there an existing baseline for user behaviour to support detection of anomalies?		Yes.
16	Section 3.1 A - SOC Monitoring	14	3.1.A	SIEM data should be correlated across sources to detect APTs and insider threats.	Are identity logs and DLP systems integrated into current SIEM?		Yes.
17	Section 3.1 A - SOC Monitoring	15	3.1.A	Log ingestion from all relevant data sources including cloud workloads is mandatory.	Can NPCI share a log source inventory by category (Infra, App, DB, Cloud)?		This will be discuss/shared with qulified bidder
18	Section 3.1 A - SOC Monitoring	15	3.1.A	Dashboards must be customized for different stakeholder groups (ISMS, audit, operations).	Is there a preferred visualization tool (e.g., Grafana, Kibana, Power BI) currently in use?		Yes.
19	Section 3.1 A - SOC Monitoring	15	3.1.A	The bidder should ensure KPI compliance with SLA targets as defined in governance review.	Please share the SLA targets expected for each incident severity level.		This will be discuss/shared with qulified bidder
20	Section 3.1 A - SOC Monitoring	15	3.1.A	Bidder must coordinate with OEMs, internal teams, and stakeholders for complex incident analysis.	Will NPCI facilitate direct coordination with third-party vendors (OEMs)?		Yes.
21	Section 3.1 B - Incident Response	15	3.1.B	Incident response should be executed within defined timelines.	What are the SLA thresholds for containment and remediation actions by severity?		This will be shared with qulified bidder
22	Section 3.1 B - Incident Response	15	3.1.B	Bidder must perform forensic analysis and prepare tamper-proof reports.	Is there an approved forensic toolkit or can bidder propose its own?		Bidder can proposed
23	Section 3.1 B - Incident Response	15	3.1.B	Bidder must simulate attacks and test controls regularly.	What is the required frequency for threat simulations?		Mutually agreed. Quterly
24	Section 3.1 B - Incident Response	16	3.1.B	Bidder must conduct root cause analysis and share lessons learned reports.	Is there a standard format for RCA documentation?		Yes.
25	Section 3.1 B - Incident Response	16	3.1.B	Incident containment should follow defined playbooks.	Will existing playbooks be shared, or is bidder responsible for creating them from scratch?		Existing playbook will shared with qulified bidder
26	Section 3.1 B - Incident Response	16	3.1.B	Must support readiness for audits and regulator checks.	Which regulatory frameworks and auditors are expected (e.g., CERT-In, RBI, PCI)?		Yes. CERT-In, RBI, PCI
27	Section 3.1 B - Incident Response	16	3.1.B	Team should conduct tabletop exercises.	Are tabletop exercises expected quarterly, semi-annually, or annually?		Semi annually

No	Section	Page No	Clause	Requirement	Query	Additional Comments	Response
28	Section 3.1 B - Incident Response	16	3.1.B	Threat actor profiling and historical pattern correlation to be performed.	Is historical threat log data available from incumbent vendor or past years?		Yes.
29	Section 3.1 B - Incident Response	16	3.1.B	Bidder must ensure evidence integrity across all phases of incident response.	Is a digital chain-of-custody tool in place?		Yes.
30	Section 3.1 B - Incident Response	16	3.1.B	Bidder shall submit monthly incident trends and response effectiveness reports.	Is there a defined incident categorization model (CVSS, internal tiering, etc.) to be followed?		Yes.
31	Eligibility - Annexure H	56		Relevant Experience in handling SOC in BFSI industry (at least 2 similar customer references in India)	Would request to have relevant Experience in handling SOC in all sectors/ BFSI / Non BFSI / industry (at least 2 similar customer references in India or Global)		BFSI refrence mandetory in India or Global
32	section 4 - Eligibility criteria	20	4.1 (1)	The bidder is a Company/ LLP registered in India under the Companies Act or Partnership under Partnership Act at least since last 3 years. a. In case the bidder is the result of a merger or acquisition, at least one of the merging companies should have been in operation for at least 2 years as on date of submission of the bid. b. In case the bidder is the result of a demerger or hiving off, at least one of the demerged company or resulting company should have been in operation for at least 2 years as on the date of submission of bid.	We would like to clarify that our organization has a strong operational presence and turnover both in UAE and India. While we have successfully completed 2 years of incorporation, we are currently in our third year of operations. We respectfully request consideration of our substantial experience and turnover across regions in support of our eligibility.	We have hereby attach our MSME Certificate , Incorporation certificate and Start up certificate and Dubai License trade certificate. Request you to Please consider the same.	No change in RFP
33	section 4 - Eligibility criteria	21	4.1 (2)	The bidder should have reported a minimum annual turnover of Rs. 20 Crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited inancial statementsn at least 2 out of the last 3 financial years (FY 2021-22,2022-23, 2023-24). In case audited financial statements for most recent financial year are not ready, then management certified financial statement shall be considered. In case the bidder is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the past financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover for the purpose of meeting the eligibility criteria; should the bidder be in operation for a period of less than 2 financial years. For this purpose, the decision of NPCI will be treated as final and no further correspondence will be entertained on this.	We would like to highlight that our organization has achieved an overall turnover of 10 crore , with established operations in both **UAE and India**. Our company is currently in its **third year of operation**, and if required, we can share the **financial documents for the assessment year 2023–2024** to support our eligibility.	Duration / Country / Turnover / INR: April 2024-March 2025, India, 88,50,000, 88,50,000; April 25 to July 25, 1,14,83,110, 1,14,83,110; Jan 2024 – Dec 2024, UAE, AED1,026,573.04, 2,46,37,752; Jan 25 to July 25, AED 2259215.56, 5,42,21,160; Total 9,91,92,022	No change in RFP
34	section 4 - Eligibility criteria	8	8	Relevant Experience in handling SOC in BFSI industry (at least 2 similar customer references in India)	We would like to clarify that while our organization is in the process of acquiring customers in the Indian BFSI sector, we do have team members with hands-on experience in managing SOC operations for BFSI clients. Given our team's domain expertise and our active efforts to establish a client base in India, we kindly request you to consider our overall experience and expertise for meeting this eligibility criterion.	We would like to highlight that our team has extensive experience in managing SOC operations, having successfully delivered multiple projects across UAE and India. Notable clients include BBK, EWEC, DWTC, Hitachi, HPE, Samsung, Tree Comma Capital, Al Ansari, and Al Rostamani. While we are currently in the process of acquiring BFSI customers specifically in India, our team includes professionals with strong experience in SOC delivery for BFSI environments. Considering our proven capabilities and solid track record, we respectfully request you to consider our overall experience as meeting the eligibility requirement.	No change in RFP

#	Section	Page	Clause	RFP Requirement	Bidder Query		NPCI Response
35	Section 3.1 - Scope of Work	13	Section - A	All daily routine and standard activities of L1 and L2 to be fully automated in phased manner within one year from the date of issuance of PO. Automation effectiveness should be measured quarterly and tracked via automation KPIs.	Type of Automation Solution Expected - Is NPCI asking the bidder to supply, implement, and maintain a dedicated automation/SOAR platform (including all licences, integrations, and runbooks)? - or Should the bidder's team leverage NPCI's existing SIEM/SOAR tool-set and focus on developing process-driven scripts/runbooks within that environment? Ownership & Licensing If a new platform is required, will NPCI procure the licences directly, or must the bidder include them in the commercial proposal? Who will retain ownership of automation workflows/runbooks after project completion? In-Scope L1/L2 Activities Please confirm the key routine tasks that must be automated (e.g., alert triage, enrichment, ticket creation/closure, report generation, containment actions, log-source health checks). A definitive list will allow us to size effort, tooling, and KPIs accurately. Baseline & KPI Targets Does NPCI have current baseline metrics for mean-time-to-respond (MTTR), false-positive rate, or manual effort hours that should be used to define quarterly automation KPIs? Are any specific audit or regulator-driven performance thresholds (e.g., RBI/NPCI guidelines) to be met? Integration Constraints Please share details of existing security stack (SIEM		Bidder should levarage existing SIEM/SOAR. Scope of L1 & L2 will be share with qulified bidder. NPCI have current baseline matrix. All regulatory audit perfomance threshold to be met e.g . RBI, PCI DSS etc. It will be share with qulified bidder.
36	Section 3.1 - Scope of Work	15	Section - B Incident Response	Resource requirement support- SOC Monitoring: Resources / Monitoring / Incident Response / Count L1 24*7 -- 8 L2 24*7 24*7 5 L3 16*5 16*5 2	L3 resource: 16 × 5 coverage may not be feasible when the primary L3 engineer is on leave.		Bidder should provide additional resource if existing L3 resources goes on leave
37	Section 3.1 - Scope of Work	16	Section - B Incident Response	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include Escalations from onsite team for specialist support on security product categories to resolve faults, configuration related issues Share best practices on product configuration standards & policies with onsite team	We would like to clarify that Alcon does not operate a dedicated SOC facility for time being. However, we can provide backend support through our Senior Security Engineer for escalations, advisory, and critical issue handling. Please confirm if this arrangement meets NPCI's requirement.		Yes.
38	Section 3.1 - Scope of Work	14	Section - B Incident Response	Bidder should prepare the SOC operations for compliance and certification to the standards of ISO 27001, ISO 20000, BS 25999 and PCI DSS.	Kindly confirm if the bidder is expected to only make the SOC operations compliant and ready for certification, or is the bidder also responsible for achieving and maintaining the actual certifications (ISO 27001, ISO 20000, BS 25999, and PCI DSS)?		No.
39	Section 4 - Eligibility Criteria	21	Relevant Experience	Relevant Experience in handling SOC in BFSI industry (at least 2 similar customer references in India)	Relevant Experience in handling SOC / Security Services in BFSI / Government / PSU (at least One similar customer references in India)		Two BFSI refrences mandatory in India or Global
40	Section 3	12	3.1	Scope of work	Could you please confirm the duration allocated for the handover process?		90 days after onboarding
41	Section 3	12	3.1	Scope of work	Could you please confirm if the handover documentation is available?		Yes.
42	Section 3	12	3.1	Scope of work	Could you please confirm the last working date of the existing vendor?		No.
43	Section 8	31	8.10	The successful bidder shall commence the services of within 6 weeks from the date of receipt of the Purchase Order (The commencement of services will be considered on at least 70% of the resources are onboarded. Remaining resources to be onboarded within 8 Weeks from date of receipt of PO).	Would it be feasible to onboard 70% of the required resources within a minimum of 8 weeks and the remaining by 12 weeks, while ensuring that the project kickoff and initial activities proceed in parallel?		No change in RFP
44	Section 3	12	3.1	Monitoring should be done on 24/7 basis with onsite personnel/resources. Bidder should provide the personnel for managing the security monitoring service as per the team specification in scope of work.	Kindly clarify whether all resources are expected to be based in Hyderabad, or if alternate/flexible locations can be explored		Between Hyderabad, Chennai, Mumbai and will be desided after onboarding of bidder
45	Section 3	15	3.1 - B	Bidder should provide inputs for coordinating with external agencies like CERT-IN, NCCC, NCIIPC and other OEMs to handle security incidents.	Is an ongoing CERT-In empanelment process acceptable, or is completed empanelment mandatory for this engagement?		No change in RFP
46	Section 3	15	3.1 - B	The SOC will be 24x7x365 environment and personal resources should be able to work in shifts and flexible working hours to support the operations.	Please clarify if standard leave policies, including holidays and weekly offs, will apply to the deployed resource. Additionally, what is the minimum capacity expected for those days?		This will be discuss with qulified bidder

47	Section 8	32	8.12	Service Level Requirements (SLA) & Penalty on non-adherence to SLAs:	Could you please confirm when the penalty clause will come into effect? Would it be possible to consider the first month as a mock or stabilization period without penalties?		Please check the clause 8.10 Delivery Schedule given in the RFP
48	Section 11	60	Point 22	Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include Escalations from onsite team for specialist support on security product categories to resolve faults, configuration related issues Share best practices on product configuration standards & policies with onsite team	In case of a backup or contingency situation, would remote access (via VPN or any other approved channel) be permitted to ensure continuity of services?		For troubleshooting purpose bidder can provide L3 support remotely to support onsite team.
49		12	3.1 Scope of work A. SOC Monitoring		What is your existing SIEM solution ? Is it on-prem deployment or on-cloud SaaS model ?		This will be discuss with qulified bidder
50		12	3.1 Scope of work A. SOC Monitoring		What is the licenses procured for your SIEM solution ?		This will be discuss with qulified bidder
51		12	3.1 Scope of work A. SOC Monitoring		What is your DC - DR setup and high availability to ensure redundancy ?		This will be discuss with qulified bidder
52		12	3.1 Scope of work A. SOC Monitoring		Number of UEBA licenses ?		This will be discuss with qulified bidder
53		12	3.1 Scope of work A. SOC Monitoring		Please explain you SIEM Platform support availability		This will be discuss with qulified bidder
54		12	3.1 Scope of work A. SOC Monitoring		What is your Peak EPS and Average observed EPS ?		This will be discuss with qulified bidder
55		12	3.1 Scope of work A. SOC Monitoring		What is the number of log sources integrated with SIEM ?		This will be discuss with qulified bidder
56		12	3.1 Scope of work A. SOC Monitoring	Bidder should monitor security logs to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in environment.	What is your tentative year-on-year increase in number of log sources integration to be factored over and above existing setup ?		This will be discuss with qulified bidder
57		12	3.1 Scope of work A. SOC Monitoring		Please share your detailed asset inventory.		This will be discuss with qulified bidder
58		12	3.1 Scope of work A. SOC Monitoring		What is the number of default and custom correlations / rules/ use cases configured		This will be discuss with qulified bidder
59		12	3.1 Scope of work A. SOC Monitoring		Average Number of possible incidents or alerts per day (Business Day and Holidays) ?		This will be discuss with qulified bidder
60		12	3.1 Scope of work A. SOC Monitoring		Please share the bifurcation of P1, P2 & P3 incidents per month ?		This will be discuss with qulified bidder
61		12	3.1 Scope of work A. SOC Monitoring		What is the ticketing tool/ ITSM used in your environment ?		This will be discuss with qulified bidder
62		12	3.1 Scope of work A. SOC Monitoring		What are your available Integrated Threat Intelligence Feeds ?		This will be discuss with qulified bidder
63		12	3.1 Scope of work A. SOC Monitoring		What is your existing number of L1, L2 & L3 analysts on 24*7 shifts ?		This will be discuss with qulified bidder

64		12	3.1 Scope of work A. SOC Monitoring		What is your SOAR platform ?		This will be discuss with qulified bidder
65		12	3.1 Scope of work A. SOC Monitoring		Please share details about the deployment model and licenses for SOAR ?		This will be discuss with qulified bidder
66		12	3.1 Scope of work A. SOC Monitoring	Bidder should add/delete/modify rules, reports and dashboards etc. on SIEM based on NPCI requirements and changing security threat landscape. Quarterly review and optimization of these elements should be mandated.	Is your SOAR integrated with SIEM & ITSM ?		Yes.
67		12	3.1 Scope of work A. SOC Monitoring		What all playbooks configured on SOAR ?		Yes.
68		12	3.1 Scope of work A. SOC Monitoring		What is the percentage of L1, L2 & L3 activities automated through SOAR ?		This will be discuss with qulified bidder
69		12	3.1 Scope of work A. SOC Monitoring		What is your existing dashboard solution ? Is it integrated with SOAR & ITSM to pull metrics in real-time ?		This will be discuss with qulified bidder
70		13	3.1 Scope of work A. SOC Monitoring	Bidder should ensure continuous training and best practice updates for onsite team from its backend resources. Training shall include updates from post-incident reviews and threat simulations	Can it be ppt/ excel / word based training ?		Yes.
71		13	3.1 Scope of work A. SOC Monitoring		What will be the mode of delivery ? (teams/ Webex/ etc) and we hope it will be provided by NPCI ?		Yes.
72		13	3.1 Scope of work A. SOC Monitoring	Bidder has to reduce the false positives on the security incidents/events. False positive rate of the incidents has to be less than 5%.	We request you to modify this clause to keep false positives within 30%, since we will also need to continuously test and implement new use cases as per evolving threats. Keeping very low false positive ratio can impact the detection capabilities.		No change in RFP
73		13	3.1 Scope of work A. SOC Monitoring	Bidder shall be responsible to develop and maintain Standard Operating Procedures (SOP) and Create / Update & maintain all playbooks with respect to SOC day to day operations including but not limited to threat management, alert/incident management, reports & dashboards, forensics infrastructure maintenance, rules creation & fine tuning, install/upgrades, updates, asset Integration, Business Continuity data & configuration backup, restoration, archival, knowledge management, segregation of duties, change management, patch & version management, KPI and KRI to measure SOC performance etc. as per policies of the NPCI.	What is your daily backup platform for configuration backups ?		This will be discuss with qulified bidder
74		13	3.1 Scope of work A. SOC Monitoring		In case of on-prem solutions, please explain the time and frequency of backups ?		This will be discuss with qulified bidder
75		13	3.1 Scope of work A. SOC Monitoring		In case of on-prem solutions, who will be responsible for managing the infra / connectivity and underlying hardware / software ?		This will be discuss with qulified bidder
76		14	3.1 Scope of work A. SOC Monitoring	Bidder should have the capability to operate and analyse NDR platform.	What is your NDR platform - make, model and version ?		This will be discuss with qulified bidder
77		14	3.1 Scope of work A. SOC Monitoring		Is it integrated with your SIEM , SOAR & ITSM ?		This will be discuss with qulified bidder
78		14	3.1 Scope of work A. SOC Monitoring		What is the traffic flow ingestion in terms of GB/Day?		This will be discuss with qulified bidder
79		14	3.1 Scope of work A. SOC Monitoring		What is the average number of P1, P2, P3 incidents generated through NDR in a month ?		This will be discuss with qulified bidder
80		14	3.1 Scope of work A. SOC Monitoring	Bidder should be able to manage multiple SIEM solutions which include open-source platforms.	Please elaborate if there are multiple SIEMs deployed in NPCI. If yes, explain the architecture.		This will be discuss with qulified bidder

81		14	3.1 Scope of work A. SOC Monitoring	Deployed resources should have knowledge of Packet capture analysis.	What is your PCAP platform - deployment model, ingestion volume and storage capacity ?		This will be discuss with qulified bidder
82		14	3.1 Scope of work A. SOC Monitoring	Deployed resources shall create Saas based alarm on GCP/AWS.	Please explain this clause. Does it mean we need to configure SIEM Usecase to detect threats on NPCI cloud instances ?		Creation of Cloud base alram is optional. But conternerized corelation workloads required from bidder side.
83		14	3.1 Scope of work A. SOC Monitoring	Deployed resources shall create Saas based alarm on GCP/AWS.	Please provide details on your cloud presence / inventory.		This will be discuss with qulified bidder
84		15	3.1 Scope of work B. Incident Response	NPCI reserves the right to interview all the personnel resources to be deployed on the project and reject if not found suitable for the project.	Since this is a SLA based contract, request you to remove the requirement of interview.		No change in RFP
85		15	3.1 Scope of work B. Incident Response	Resource requirement support- SOC Monitoring:	You have asked for 15 resources onsite ? How should we factored leave reliver ? Will it be over and above this requirement ? If the requirement of onsite resources increases due to increase on ingestion volume, incidents, workload, etc,. How it will be factored and provided to NPCI ?		Yes. No. Basis on workload will increase additional manpower as per contract
86		16	3.1 Scope of work B. Incident Response	22. Bidder should provide backend support to the onsite team from its own SOC. Such support at the minimum include Escalations from onsite team for specialist support on security product categories to resolve faults, configuration related issues Share best practices on product configuration standards & policies with onsite team	Since this is entire onsite resource deployment, what is the resource factorization to be done for remote support ?		Yes.
87		16	3.1 Scope of work B. Incident Response		Please explain if NPCI will allow remote access to its SIEM, SOAR and other SOC solutions ?		No
88		16	3.1 Scope of work B. Incident Response		Will NPCI provide IPSec VPN connectivity for remote access ?		Yes. On NPCI laptops
89		16	3.1 Scope of work B. Incident Response	23. Firewall Rule base review to be done using provided tool and consecutively coordinating with application owner/team	What is the number of firewalls, make and model to be considering to size the efforts ?		This will be discuss with qulified bidder
90		16	3.1 Scope of work B. Incident Response		What is the required frequency of reviews (Quarterly, Half yearly/ Annually) ?		Quarterly
91		17	3.1 Scope of work B. Incident Response	15. NPCI reserves the right to audit Bidder either by itself or through any appointed entity. Bidder must provide full cooperation for audit of services in the scope of this Purchase Order.	Since this is an onsite resource supply requirement, what is NPCI scope under security audit of bidder SOC ?		This will be discuss with qulified bidder
92		19	3.1 Scope of work B. Incident Response	Manpower Requirement:	Please share the bifurcation of L1, L2, L3 requirements at NPCI DC & DR.		This will be discuss with qulified bidder
93		20	4.1 Eligibility Criteria	Turnover & profitability: The bidder should have reported a minimum annual turnover of Rs. 50 Crores	Request you to increase the turnover criteria to a minimum of 200 Crores.		No change in RFP
94		26	5.25 Bid Evaluation Process	Stage 2 –Folder 'C' of those Bidders who qualify the eligibility and technical criteria will be evaluated. NPCI reserves the right to conduct Reverse Auction (RA) or Price discussion mechanism to arrive the exact price and successful bidder	Request you to consider modification in selection criteria (QCBS), since L1 through reverse auction may impact the quality of resources deployed.		No change in RFP
95		28	7.3 Technical Scoring Matrix	Technical Scoring Matrix:	The scoring marks are not mentioned in RFP, can you please provide the weightage assigned to each evaluation parameter.		Will share in Corrigendum 1
96		32	8.12 Service Level Requirements (SLA) & Penalty on non-adherence to SLAs:	Content development and Creation of use cases	We request exclusion of parsers which has OEM dependency for creation.		No change in RFP

97		34	8.12 Service Level Requirements (SLA) & Penalty on non-adherence to SLAs:	Availability and Configuration Management	We request exclusion of uptime SLA for cases which has dependency on underlying infra - hardware and software or OEM ?		No change in RFP
98	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	25	5.23	**5.23 Right to Reject, Accept/Cancel the bid** NPCI reserves the right to accept or reject, in full or in part, any or all the offers without assigning any reason whatsoever. NPCI does not bind itself to accept the lowest or any tender and reserves the right to reject all or any bid or cancel the Tender without assigning any reason whatsoever. NPCI also reserves the right to re-issue the Tender without the Bidders having the right to object to such re-issue.	**We propose changes in the existing clause as below:-** **Right to Reject,Accept/Cancel the bid:-** NPCI reserves the right to accept or reject, in full or in part, any or all the offers without assigning any reason whatsoever, subject to legal and regulatory requirements. NPCI does not bind itself to accept the lowest or any tender and reserves the right to reject all or any bid or cancel the Tender without assigning any reason whatsoever. NPCI also reserves the right to re-issue the Tender without the Bidders having the right to object to such re-issue,as long as such re-issue complies with applicable legal obligations.		No change in RFP
99	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	36	8.21	8.21 Confidentiality	**As mentioned in the clause no. 8.21 Confidentiality i.e :-The Successful bidder shall execute separate NDA on the lines of the format provided in the Annexure Z hereof.** However, we could not find any such Annexure attached. Kindly provide the same.		There is no such NDA document, it's a typo error
100	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	37	8.23	**8.23 Liability** Bidder's Liability: The Bidder's liability in case of claims against NPCI resulting from willful and gross misconduct, or gross negligence, fraud of the Bidder, its employees, contractors and subcontractors, from infringement of patents, trademarks, and copyrights or other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited.	**We propose changes in the existing clause as below:-** **Liability:-** **Bidder's Liability:** The Bidder's liability in case of claims against NPCI resulting from willful and gross misconduct, or gross negligence, fraud of the Bidder, its employees, contractors and subcontractors, from infringement of patents, trademarks, and copyrights or other Intellectual Property Rights or breach of confidentiality obligations shall be unlimited,provided that such liability shall arise only upon final determination by a court of competent jurisdiction or as required under applicable law, and subject to principles of natural justice and due process.		No change in RFP
101	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	37	8.25	**8.25 Exit option and contract re-negotiation** a)NPCI reserves its right to cancel the order in the event of happening of one or more of the situations as mentioned in the "Order Cancellation" herein under. b) Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder should continue to provide the facilities to NPCI at NPCI's locations. c) Reverse transition mechanism would be activated in the event of cancellation of the contract or exit by the bidders prior to expiry of time for awarding the final bid / the contract. The Bidder should perform a reverse transition mechanism to NPCI or its selected bidder. The reverse transition mechanism would facilitate an orderly transfer of services to NPCI or to an alternative 3rd party / bidder nominated by NPCI. Where NPCI elects to transfer the responsibility for service delivery to a number of bidders, NPCI will nominate a bidder who will be responsible for all dealings with the Bidder regarding the delivery of the reverse transition services. d) The reverse transition services to be provided by the Bidder shall include the following: i. The Bidder shall suitably and adequately train NPCI or its designated team for fully and effectively manning, operating the Devices. ii. Bidder shall provide adequate documentation thereof. iii. The Bidder shall jointly manage the Devices with NPCI or designated team for a reasonable period of time e) Knowledge Transfer: The Bidder shall provide such necessary information, documentation to NPCI or its designee, for the effective management and maintenance of the Deliverables	**We propose changes in the existing clause as below:-** **Exit option and contract re-negotiation:-** a)NPCI reserves its right to cancel the order in the event of happening of one or more of the situations as mentioned in the "Order Cancellation" herein under,subject to prior written notice and reasonable opportunity for the Bidder to cure any alleged breach. b) Notwithstanding the existence of a dispute, and/or the commencement of arbitration proceedings, the Bidder should continue to provide the facilities to NPCI at NPCI's locations, provided that NPCI continues to fulfill its corresponding payment and contractual obligations during such period. c) Reverse transition mechanism would be activated in the event of cancellation of the contract or exit by the bidders prior to expiry of time for awarding the final bid / the contract. The Bidder should perform a reverse transition mechanism to NPCI or its selected bidder. The reverse transition mechanism would facilitate an orderly transfer of services to NPCI or to an alternative 3rd party / bidder nominated by NPCI. Where NPCI elects to transfer the responsibility for service delivery to a number of bidders, NPCI will nominate a bidder who will be responsible for all dealings with the Bidder regarding the delivery of the reverse transition services,subject to mutually agreed timelines, scope, and commercially reasonable efforts by the Bidder. d) The reverse transition services to be provided by		No change in RFP

102	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	38	8.26	**8.26 Extension of Contract** The bidder shall be required to consistently execute, in a successful and professional manner, the jobs assigned under this RFP or subsequent Purchase Order / Contract, as shall be entered by NPCI with the Bidder, to the satisfaction of and as decided by the NPCI up to a period of three (3) years (completion period) reckoned from the date of commencement of the services and may be extended for further period on satisfactory performance by bidder. However even in case, the bidder is not interested to extend the Contract for a further period, bidder shall be essentially required to execute the work at least for next 6 months' period on the same rates and terms & conditions of the Contract. NPCI has right to alter (increase or decrease) the number of resources. NPCI has right to place repeat order to the bidder for any resources mentioned in the Contract. The contract shall be co-terminus with the Purchase orders issued unless extended by NPCI.	**We propose changes in the existing clause as below:-** **Extension of Contract** The bidder shall be required to consistently execute, in a successful and professional manner, the jobs assigned under this RFP or subsequent Purchase Order / Contract, as shall be entered by NPCI with the Bidder, to the satisfaction of and as decided by the NPCI up to a period of three (3) years (completion period) reckoned from the date of commencement of the services and may be extended for further period on satisfactory performance by bidder,as mutually agreed between the Parties. However even in case, the bidder is not interested to extend the Contract for a further period, bidder shall be essentially required to execute the work at least for next 6 months' period on the same rates and terms & conditions of the Contract,unless otherwise mutually agreed. NPCI has right to alter (increase or decrease) the number of resources ,subject to mutual agreement wherever commercially or operationally significant. NPCI has right to place repeat order to the bidder for any resources,on mutually agreed terms & conditions as mentioned in the Contract. The contract shall be co-terminus with the Purchase orders issued unless extended by NPCI.		No change in RFP
103	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	38	8.27	**8.27 Order Cancellation** NPCI reserves its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to NPCI alone; i. Delay in delivery is beyond the specified period as set out in the Purchase Order before acceptance of the product; or, ii. Serious discrepancy in the quality of service expected. iii. If a Bidder makes any statement or encloses any form which turns out to be false, incorrect and/or misleading or information submitted by the bidder turns out to be incorrect and/or bidder conceals or suppresses material information. In case of order cancellation, any payments made by NPCI to the Bidder for the particular service would necessarily have to be returned to NPCI with interest @ 15% per annum from the date of each such payment. Further the Bidder would also be required to compensate NPCI for any direct loss incurred by NPCI due to the cancellation of the Purchase Order and any additional expenditure to be incurred by NPCI to appoint any other Bidder. This is after repaying the original amount paid.	**We propose changes in the existing clause as below:-** **Order Cancellation:-** NPCI reserves its right to cancel the order in the event of one or more of the following situations, that are not occasioned due to reasons solely and directly attributable to NPCI alone;by providing prior written notice of 15 days and a 30 day's cure period to the Bidder to rectify such default. i. Delay in delivery is beyond the specified period as set out in the Purchase Order before acceptance of the product; or, ii. Serious discrepancy in the quality of service expected,as objectively measured against agreed service levels and mutually defined technical specifications. iii. If a Bidder makes any statement or encloses any form which turns out to be false, incorrect and/or misleading or information submitted by the bidder turns out to be incorrect and/or bidder conceals or suppresses material information. In case of order cancellation, any payments made by NPCI to the Bidder for the particular service would necessarily have to be returned to NPCI with interest @ 15% per annum from the date of each such payment. Further the Bidder would also be required to compensate NPCI for any direct loss incurred by NPCI due to the cancellation of the Purchase Order and any additional expenditure to be incurred by NPCI to appoint any other Bidder. This is after repaying the		No change in RFP

104	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	39	8.28	**8.28 Termination of Purchase Order/Contract** For Convenience: NPCI, by written notice sent to Bidder, may terminate the Purchase Order/ contract in whole or in part at any time for its convenience giving three months' prior notice. The notice of termination may specify that the termination is for convenience the extent to which Bidder's performance under the contract is terminated and the date upon which such termination become effective. NPCI shall consider request of the bidder for pro-rata payment till the date of termination. For Insolvency: NPCI at any time may terminate the contract by giving written notice to Bidder, if Bidder becomes bankrupt or insolvent. In this event, termination will be without compensation to Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to NPCI. For Non-Performance: NPCI reserves its right to terminate the contract in the event of Bidder's repeated failures (say more than 3 occasions in a calendar year to maintain the service level prescribed by NPCI).	**We propose changes in the existing clause as below:-** **Termination of Purchase Order/Contract** **For Convenience:** NPCI, by providing 90 day's prior written notice sent to Bidder, may terminate the Purchase Order/ contract in whole or in part at any time for its convenience giving three months' prior notice. The notice of termination may specify that the termination is for convenience the extent to which Bidder's performance under the contract is terminated and the date upon which such termination become effective. NPCI shall consider request of the bidder for pro-rata payment till the date of termination. **For Insolvency:** NPCI at any time may terminate the contract by giving written 30 day's prior notice to Bidder, if Bidder becomes bankrupt or insolvent. In this event, termination will be without compensation to Bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to NPCI. **For Non-Performance:** NPCI reserves its right to terminate the contract in the event of Bidder's repeated failures (say more than 3 occasions in a calendar year to maintain the service level prescribed by NPCI).		No change in RFP
105	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	39	8.28	Addition of new clause under the existing clause of 8.28 Termination of Purchase Order/Contract:-	**We reccomend to add new clause under the existing clause of termination as below:-** **Termination of Purchase Order/Contract:-** **For Temination by the bidder for breach:-** In the event NPCI materially breaches this definitive Agreement or any statement of work, which breach is not cured within thirty (30) days after written notice specifying the breach is given to the NPCI, the bidder may terminate this defenitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the NPCI.		No change in RFP
106	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	39	8.29	**8.29 Effect of Termination** • The Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment. • Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services •The Bidder agrees that after completion of the Term or upon earlier termination of the assignment the Bidder shall, if required by NPCI, continue to provide facility to NPCI at no less favorable terms than those contained in this RFP. In case NPCI wants to continue with the Bidder's facility after the completion of this contract then the Bidder shall offer the same terms to NPCI. •NPCI shall make such prorated payment for services rendered by the Bidder and accepted by NPCI at the sole discretion of NPCI in the event of termination, provided that the Bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be admissible. There shall be no termination compensation payable to the Bidder. •NPCI may make payments of undisputed amounts to the Bidder for services rendered till the effective date of termination. Termination shall be without prejudice to any other rights or remedies NPCI may be entitled to hereunder or at law and shall not affect any accrued rights or liabilities or either party nor the coming into force or continuation in force of any provision hereof which is expressly intended to come	**We propose changes in the below clause as below:-** **Effect of Termination:-** • The Bidder agrees that it shall not be relieved of its obligations under the reverse transition mechanism notwithstanding the termination of the assignment. • Same terms (including payment terms) which were applicable during the term of the contract should be applicable for reverse transition services,unless otherwise mutually agreed in writing by both parties considering the nature and duration of such services. •The Bidder agrees that after completion of the Term or upon earlier termination of the assignment the Bidder shall, if required by NPCI, continue to provide facility to NPCI at no less favorable terms than those contained in this RFP. In case NPCI wants to continue with the Bidder's facility after the completion of this contract then the Bidder shall offer the same terms to NPCI, ubject to mutual agreement and commercial feasibility. •NPCI shall make such prorated payment for services rendered by the Bidder and accepted by NPCI at the sole discretion of NPCI in the event of termination, provided that the Bidder is in compliance with its obligations till such date. However, no payment for "costs incurred, or irrevocably committed to, up to the effective date of such termination" will be admissible. There shall be no termination compensation payable to the Bidder. •NPCI may make payments of undisputed amounts to		No change in RFP

107	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	41	8.36	**8.36 Solicitation of Employees** Both NPCI & successful Bidder the Parties should agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties should agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge to directly or indirectly solicit of this contract for employing the key personnel working on the project contemplated in this proposal except with the written consent of the other party. The above restriction would not apply to either party for hiring such key personnel who (i) initiate discussions regarding such employment without any direct or indirect solicitation by the other party (ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or (iii) has been terminated by a party prior to the commencement of employment discussions with the other party.	**We propose changes in the existing clause as below:-** **Solicitation of Employees:-** Both NPCI and the successful Bidder (collectively, the "Parties") agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this Agreement during the period of the contract and one year thereafter, except as the Parties may agree on a case-by-case basis, and only with the prior written consent of the other Party. The Parties agree that for the period of the contract and one year thereafter, neither Party will cause or permit any of its directors or employees who have knowledge of or were exposed to the employees of the other Party in connection with this contract to directly or indirectly solicit for employment any of the key personnel working on the project contemplated in this proposal, or aid any third party in doing so, except with the written consent of the other Party. The above restriction would not apply to either Party for hiring such key personnel who: •(i) initiate discussions regarding such employment without any direct or indirect solicitation by the other Party; •(ii) respond to any public advertisement placed by either Party or its affiliates in a publication of general circulation; or •(iii) have been terminated by a Party prior to the commencement of employment discussions with the		No change in RFP
108	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	30	8.4	The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG)	The Successful bidder shall, within 30 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 5% of total value of the Purchase order (exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG)		No change in RFP
109	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	28	7.3	Technical Scoring Matrix	Kindly request NPCI to confirm the scores allocated for each section.		Scores are internal to NPCI hence cant be disclosed
110	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	12	3.1 Scope of work: A. SOC Monitoring	Team should send customized alerts and advisories about the latest CVEs and latest threats getting exploited in the cyber world, to respective teams in NPCI. Bidder should also provide the latest threat advisories to NPCI on daily basis.	**Request for Clarification:** Could you please confirm the exact objective we need to achieve regarding the latest CVEs and exploited threats? Additionally, please clarify whether you are currently receiving IOCs from third-party vendors or government entities.		This will be discuss with qulified bidder
111	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	13	3.1 Scope of work: A. SOC Monitoring	On quarterly basis, Bidder should conduct table top or CTF events within the team to enhance the knowledge levels of L1/L2/L3 and deployed NPCI resources. Each event should include metrics for evaluation and lessons learned review.	**Request for Clarification:** As per the clause, the bidder is required to conduct CTF or Tabletop exercises. There are a few products available that offer such capabilities. Should we consider including a product for this purpose, or can we propose a manual approach using threat scenarios simulated with the existing technologies available within NPCI?		Bidder can levarage the available platform of NPCI to train the team on periodic basis to upscale the knowledge.
112	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	13	3.1 Scope of work: A. SOC Monitoring	Bidder shall perform digital forensic investigation on need basis with complete replay of attack including the ingress and egress of payload. Provide complete insight into threat vector and impact analysis with detailed RCA.	**Request for Clarification:** Digital forensics will be conducted by industry professionals with expertise in breach investigations and comprehensive threat management. Can we factor in a certain number of hours for digital forensic support over the contract period, allowing NPCI to utilize them as needed?		Its optional.
113	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	14	3.1 Scope of work: A. SOC Monitoring	Bidder should provide appropriate training to deployed resources	**Request for Clarification:** Could you please confirm whether the training needs to be delivered by the OEM directly, or if it can be conducted by bidder-certified resources? Additionally, kindly confirm the number of training days for OEM Training?		By Bidder number of days will discuss mutually

114	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	14	3.1 Scope of work: B. Incident Response	Bidder should conduct security trainings for NPCI nominated persons once in six months. The training program would cover mutually agreed agenda on the e-security products and technologies.	**Request for Clarification:** Could you please confirm whether the training needs to be delivered by the OEM directly, or if it can be conducted by bidder-certified resources? Additionally, kindly confirm the number of training days and the expected number of participants from NPCI		By Bidder number of days will discuss mutully
115	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	15	Technical/Service Specification:	23. Firewall Rule base review to be done using provided tool and consecutively coordinating with application owner/team.	**Request for Clarification:** As per the clause, the bidder is required to perform a firewall rule review using a tool. There are several OEM solutions available that provide this functionality. Could you please clarify if we are expected to propose a new tool for firewall rule review, or if the customer has a different approach in mind? Additionally, please confim if customer is already using some tool for this. please specify the tool name.		NPCI have own firewall rule tool. Tool name will share with qulified bidder.
116	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	What is the Exact EPS to be consumed by the SIEM			This will be shared with qulified bidder.
117	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	How many locations does SIEM should collects log from & how many eps expected from each location with unique log source types ?			This will be shared with qulified bidder.
118	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Is it possible to get the details on the applications expected to be integrated with SIEM? This is to verify the number of custom parsers to be built?			This will be shared with qulified bidder.
119	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Name of the service desk currently in use			This will be shared with qulified bidder.
120	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Approx. number of cases raised by SOC per week			This will be shared with qulified bidder.
121	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Approx. number of alerts triggered in SIEM per week			This will be shared with qulified bidder.
122	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Total Devices integrated with SIEM (Please share the inventory with type and count)			This will be shared with qulified bidder.
123	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Kindly Mentioned the Geolocation for On-Prem (where onsite resources to be deployed)			This will be shared with qulified bidder.
124	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	what will be the Contract time period for the dedicated resource at your location?			3 Years
125	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Kindly Specify the ticketing tool integrated with SIEM Solution?			This will be shared with qulified bidder.
126	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Does the log sources include any cloud deployments (Azure, AWS , GCP and any other) to be integrated? If yes, please share the details of them?			This will be shared with qulified bidder.
127	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Does customer own log retention as part of SOC? Or what is the approach?			Yes log reteaintion is there in NPCI
128	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	What is the number of Log sources / devices integration that you would forecast during the contract period? Provide a yearly or quarterly break up along with inventory type?			This will be shared with qulified bidder.
129	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	What are the security products to used by IR team for investigation			This will be shared with qulified bidder.
130	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	What is expected log retention Period? Please specify the Online and Offline Retention periods along with archival timelines?			This will be shared with qulified bidder.
131	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	what are the use cases customer is looking to address with SIEM solution, primarily is it compliance, Threat detection or Analytical capability?			This will be shared with qulified bidder.
132	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	A part from SIEM any other security platfomer is expected to manage by bidder ?			SIEM, SOAR, NDR and UEBA
133	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Threat-hunting cadence – The RFP mentions continuous threat hunting; please clarify NPCI's minimum expectation (e.g., one hypothesis-based hunt per week / month).			This will be discuss with qulified bidder
134	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Automation target – The document states "automate all routine L1/L2 tasks within 12 months." Please list at least five tasks NPCI considers "routine" for baseline alignment			This will be shared with qulified bidder.
135	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Can bidder propose the number of resource require or it has to be as per RFP mentioned team count			No.
136	NPCI/RFP/2025-26/IT/06	12	SOW 3.1	Transition-in timeline – The schedule states 70 % resource deployment within six weeks. Is this counted from LOI, PO, or VPN access date?			From date of PO release
137		60	Technical/Service Specification	Take the backup of product configuration files any time there is a change in device configuration	Need to understand services scope		This will be shared with qulified bidder.

#	RFP Reference	Clause	Section	RFP Clause	Query		Response
138		17	Other Requirements	Bidder should prepare the SOC operations for compliance and certification to the standards of ISO 27001, ISO 20000, BS 25999 and PCI DSS.	Kindly clarfiy what areas needs to be covered in this preparation.		Compliance of this certifiation
139		15	Resource requirement support- SOC Monitoring	Number of resources	the resource count given is to be deployed in PR and DR or only PR.		Hyderabad, Chennai Mumbai & will mutually discuss with qulified bidder
140		14	Scope pf work	Bidder should have the capability to perform API-based integration with cloud-based platforms with existing SIEM solutions.	Which SIEM tool is curretly deployed.		This will be shared with qulified bidder.
141		15	Scope pf work	Bidder should be able to manage multiple SIEM solutions which include open-source platforms.	What SIEM platforms are currently being used.		This will be shared with qulified bidder.
142				[table: Duration / Country / Turnover / INR — April 2024-March 2025 India 88,50,000 / 88,50,000; April 25 to July 25 1,14,83,110 / 1,14,83,110; Jan 2024 - Dec 2024 UAE AED1,026,573.04 / 2,46,37,752; Jan 25 to July 25 AED 2259215.56 / 5,42,21,160; Total 9,91,92,022] ...ul bidder shall commence the services of within 6 ...he date of receipt of the Purchase Order	As per industry standards, a minimum of 120 days is typically required to shortlist, interview, and onboard L2 and L3 resources to ensure the right expertise and skillsets are aligned with the project requirements.		No change in RFP
143		32	Content development and Creation of use cases	For any unparsed event, parser creation should be done in SIEM within 1 week.	What are the expectations around parser development – frequency, turnaround time, and support from OEMs as 1 week can be challenging I certain scenarios		No change in RFP
144			General Queries		Can you provide a **sample** SLA compliance and SOC performance dashboard/report?		This will be shared with qulified bidder.
145					Will the deployed resources be required to work in NPCI's own security tools, or is the bidder allowed to propose alternate tooling?		On NPCI's Own security tools
146					Can NPCI confirm if infrastructure and software licenses (SIEM, SOAR, ticketing tools) will be provided by NPCI or bidder is expected to provision?		This will be shared with qulified bidder.
147					Will any knowledge base or documentation from the existing vendor be provided to the incoming bidder?		Yes.
148	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	14	A. SOC Monitoring	Bidder should be able to manage multiple SIEM solutions which include open-source platforms.	Could you please confirm the SIEM solution currently deployed in NPCI's environment?		This will be shared with qulified bidder.
149	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	NA	A. SOC Monitoring	General	What is the approximate Events Per Second (EPS) rate and/or total monthly log volume being processed?		This will be shared with qulified bidder.
150	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	14	A. SOC Monitoring	Bidder should be able to manage multiple SIEM solutions which include open-source platforms.	Is the existing SIEM infrastructure managed internally by NPCI or outsourced to a third-party vendor?		This will be shared with qulified bidder.
151	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	12	A. SOC Monitoring	Monitoring should be done on 24/7 basis with onsite personnel/resources. Bidder should provide the personnel for managing the security monitoring service as per the team specification in scope of work.	At which NPCI office locations are the on-site SOC personnel expected to be stationed?		Hyderabad, Chennai Mumbai & will mutually discuss with qulified bidder
152	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	14	A. SOC Monitoring	Bidder should be able to manage multiple SIEM solutions which include open-source platforms.	Will the selected vendor be responsible for managing the SIEM platform, including tasks such as break-fix support, upgrades, patching, and onboarding/offboarding of log sources?		Yes
153	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	NA	Genral	NA	Is the vendor permitted to propose an MXDR platform as a supplementary detection layer that ingests alerts from the existing SIEM, correlates with threat intelligence and telemetry, and enables enriched threat detection and incident creation?		No.
154	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	14	A. SOC Monitoring	Bidder should have strong knowledge to implement / improvise existing SOAR solutions and create playbooks for workflow automation. SOAR runbooks shall be measured for performance, coverage, and execution success rates.	Has a SOAR platform already been implemented in NPCI's current setup? If not, can the vendor propose and integrate SOAR capabilities along with their MXDR offering?		This will be discuss with qulified bidder
155	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	NA	A. SOC Monitoring	General	If the vendor's MXDR and/or SOAR platform is approved, will NPCI provide the required virtual infrastructure (VMs), or is the vendor expected to provision and manage it?		NPCI will provide
156	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	13	A. SOC Monitoring	Bidder shall perform digital forensic investigation on need basis with complete replay of attack including the ingress and egress of payload. Provide complete insight into threat vector and impact analysis with detailed RCA.	Do you require support limited to incident triage, or full response and containment for all incidents?		full response and containment for all incidents

157	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	13	A. SOC Monitoring	General	Is there a requirement for Forensic Retainer Services? If so, please specify the number of hours expected.		Optional
158	NPCI/RFP/2025-26/IT/06 dated 09th July 2025	NA	NA	General	Will the vendor be responsible for managing or supporting any third-party security tools (e.g., Firewalls, EDR/XDR platforms) as part of the SOC engagement?		No.
159	RFP - Scope of Work	15	B. Incident Response	Resource requirement support- SOC Monitoring: L1, L2, L3	Can the proposed team be changed, or is it fixed? Can we include a SOC Manager in the team?		This will be discuss with qulified bidder
160	RFP - Scope of Work	14	A. SOC Monitoring	The bidder should have capable resources to work on NPCI's SIEM existing platform.	Where is the SOC team located? Is it in a single location or spread across multiple sites? Do you have an existing forensic team in place, or would you like us to propose one?		Hyderabad, Chennai Mumbai & will mutully discuss with qulified bidder
161	3.1 Scope of Work – SOC Monitoring	12			What are the existing SIEM platforms in use at NPCI? Are there any expectations to migrate or integrate with new SIEM tools during the contract?		This will be discuss with qulified bidder
162	3.1 Scope of Work – SOC Monitoring	12			Is there a predefined list of log sources and formats for onboarding, or should the bidder anticipate identifying and onboarding additional sources?		predefined list of log sources and format available
163	3.1 Scope of Work – SOC Monitoring	13			Regarding the automation of L1/L2 activities within a year, is there a preferred SOAR tool already implemented or should the bidder propose one?		SOAR platform already there
164	3.1 Scope of Work – SOC Monitoring	13			Could you provide clarity on how many SIEMs and their types are currently operational?		This will be discuss with qulified bidder
165	3.1 Scope of Work – SOC Monitoring	13			Is NPCI currently using any NDR (Network Detection and Response) platform? If yes, please specify which one, and the expected responsibility of the MSSP.		This will be discuss with qulified bidder
166	3.1 Scope of Work – SOC Monitoring	13			Is there an existing MITRE ATT&CK mapping for use cases, or should the bidder build and maintain it from scratch?		MITRE ATT&CK mapping is available
167	3.1 Scope of Work – SOC Monitoring	14			Could NPCI provide a high-level architecture of the current security technology stack including EDR, NDR, SOAR, SIEM, firewalls, IDS/IPS, etc.?		This will be discuss with qulified bidder
168	3.1 Scope of Work – SOC Monitoring	14			What cloud platforms are in use (e.g., GCP, AWS, Azure)? What are the specific expectations from MSSP for cloud-native threat monitoring?		This will be discuss with qulified bidder
169	3.1 Scope of Work – SOC Monitoring	14			What tools or infrastructure is used for packet capture analysis? Is full-packet capture already in place?		This will be discuss with qulified bidder
170	3.1 Scope of Work – SOC Monitoring	14			Does NPCI have an existing threat intelligence platform or subscriptions (e.g., MISP, Anomali)?		Yes.
171	3.1 Scope of Work – SOC Monitoring	15			Are there any templates or compliance-driven formats that the MSSP must use for reports? How many different types of reports are expected on a daily/weekly/monthly basis?		This will be discuss with qulified bidder
172	3.1 Scope of Work – SOC Monitoring	15			Are there existing baseline metrics (MTTD, MTTR, False Positive Rate, Analyst Efficiency Index) available for transition?		Yes.
173	3.1 Scope of Work – SOC Monitoring	15			What secure evidence repository is available or should the MSSP propose one? How long must forensic evidence be retained?		This will be discuss with qulified bidder
174	3.1 Scope of Work – Resource Requirement	18			Can you confirm the timelines for onboarding approval by NPCI for proposed L1/L2/L3 resources?		Please check the clause 8.10 Delivery Schedule given in the RFP
175	3.1 Scope of Work – Resource Requirement	18			Are all SOC resources expected to be on-premise at NPCI locations? Or is there flexibility for a hybrid model?		Only Onsite
176	3.1 Scope of Work – Resource Requirement	18			Will NPCI provide test/interview criteria for periodic technical evaluations of deployed MSSP staff?		Yes.
177	3.1 Scope of Work – Process & Governance	17			Will MSSP follow NPCI's internal change management process or implement its own for SOC changes (e.g., rule tuning, parser updates)?		Yes.
178	3.1 Scope of Work – Process & Governance	17			What is the expected timeline to submit RCA for critical incidents? Should it follow a predefined format?		This will be discuss with qulified bidder
179	3.1 Scope of Work – Process & Governance	17			What types of audits (internal, CERT-In, RBI, ISO) are planned during the contract period? What level of audit participation is expected?		RBI , Cert - in , ISO, PCI DSS, SOC 2 etc. Highest auidt participation is expected

#	Section	Page	Clause		Query		Response
180	3.1 Scope of Work – Process & Governance	17			Will NPCI provide tools or scenarios for tabletop exercises, or is the MSSP expected to design and execute simulations?		NPCI will provide
181	Section 4 – Eligibility Criteria	20			For a company registered under the MSME Act with complete technical capabilities as per RFP requirements, but not meeting the 3-year operation or turnover threshold—can such a company still bid under any exemption or special consideration?	Clarification on MSME eligibility for technically competent but newly registered companies.	No change in RFP
182	Section 4 – Eligibility Criteria				Kindly confirm whether participation in the form of a Consortium or Joint Venture is permitted for this tender		No change in RFP
183	Section 4 – Eligibility Criteria	21	Clause #8 Relevant Experience	Relevant Experience in handling SOC in BFSI industry (at least 2 similar customer references in India)	Relevant Experience in Security Solution Implementation/handling SOC in BFSI/Private industry (at least 2 similar customer references in India)		Two BFSI refrence mandetory in India or Global
184	Section 3 – Scope of Work	19	Clause #3.1	Manpower Requirement	Please confirm on per shift requirement for L1. L2 & L3 Resources for resource planning to meet the SLA defined in RFP		No change in RFP
185	Additional	NA	NA		The aggregate liability of the selected bidder for all penalties, liquidated damages, or service credits arising under this RFP and the resultant agreement shall not exceed 10% of the total contract value.		No change in RFP
186	Section 8 –Terms and Conditions	30	Clause #8.4	The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG)	Request for reduction of PBG from 10% to 3%.	As per Ministry of Defence, Office Order dated 14.01.2022 for implementation of reduction of PWBG from 5-10% to 3% of the value of contract.	No change in RFP
187	Section 3 – Scope of Work	24	Clause #5.14		Declaration of Clean Track Record by OEM – Annexure D		No change in RFP
188	Section 3.1, SIEM and SOAR platform	12-15			Please clarify Deployed SIEM platform and SOAR platform		This will be discuss with qulified bidder
189	Section 3.1, SIEM and SOAR platform	12-15			Whether SIEM and SOAR solutions are running on-prem or on cloud?		This will be discuss with qulified bidder
190	Section 3.1, SIEM and SOAR platform	12-15			How much is the EPS of SIEM platform?		This will be discuss with qulified bidder
191	Section 3.1, SIEM and SOAR platform	12-15			How many log sources are integrated with SIEM platform		This will be discuss with qulified bidder
192	Section 3.1, SIEM and SOAR platform	12-15			Please share alert count of last 6 months		This will be discuss with qulified bidder
193	Section 3.1, SIEM and SOAR platform	12-15			Please share true positive ratio of last 6 months		This will be discuss with qulified bidder
194	Section 3.1, SIEM and SOAR platform	12-15			Please share existing service request data to provide insight of parser cration requests per month.		This will be discuss with qulified bidder
195	Scope of work and SLAs Team size and roles	15, 32			RFP has defined SLAs for SIEM operations, engineering activities, threat intelligence, threat hunting etc. Where as team structyre is defined with L1, L2 and L3 roles with count. Team size appears to be insufficient in view of scope and resource count. please clarify whether bidder is allowed to structure team size as appropriate and how NPCI will consider the same?		No.
196	SLAs and other deliverables	32			To meet objectives of NPCI, whether bidder can position own assets for performing work efficiently and how NPCI will evaluate the same?		No.
197	Section 8.12	33			Kindly confirm whether NPCI is having Threat Intel Feed that can be leverage by SOC Team		Yes
198	Section 8.12	33			Does NPCI has a TIP Platform		Yes
199	Section 8.12 (Architecture and solution planning, reviewing & designing)	34			How many service request has been raised in last 6 months for Architect review.		This will be discuss with qulified bidder
200	Section 8.12 (Policy & user Management)	34			How many service request has been raised in last 6 months for Policy and User Management.		This will be discuss with qulified bidder
201	Section 8.12 (Forensic Investigation)	34			Does NPCI has subscribed any third Party forensic services or Bidder should provide/Include forensic services		This will be discuss with qulified bidder
202	Section 7.3 (Technical Scoring Matrix)	28			Please sepcifie Scores in technical score matrix		will provide in Corrgendum 1

#	Section	Page	Ref	Clause	Query		Response
203	Section 8.12 (Penalty SLA)	32			Penalty clause should be within capping range of 5% of quarterly invoice value		No change in RFP
204	Section 8.23 - (Liability)	37			we request to remove unlimited liability or it should be capping of 10% of quarterly invoice value		No change in RFP
205	Section 9 - (Technical Skill set)	43			Requesting NPCI to confirm L1,L2 & L3 resource profile		This will be discuss with qulified bidder
206	NDR Platform (Network Detection and Response)	14			Requesting to know, Which NDR Platform is being used at NPCI		This will be discuss with qulified bidder
207	Section 8.12 (Integration of assets with SIEM and Event Monitoring)	32			Request NPCI to share average incidents per month with its Severity / priority with MTTR? (i.e. P1, P2, P3)		This will be discuss with qulified bidder
208	Section 8.12 (Content development and Creation of use cases)	32			Does NPCI has application inventory available for which custom Parcer needs to be built?		This will be discuss with qulified bidder
209	Section 8.11 (Penalty for default in delivery)	31			In case the delay exceeds 10 days beyond the stipulated delivery period of RFP, " Request to increase time lines from 10 days to 30 days"		No change in RFP
210	Section 8.12 (Content development and Creation of use cases)	32			Total number of use cases Count (Default & Custom) running in SIEM		This will be discuss with qulified bidder
211	Section 3.1 (A. SOC Monitoring)	14			Total Number of play books in SOAR		This will be discuss with qulified bidder
212	Section 8.12 (Integration of assets with SIEM and Event Monitoring)	32			Kindly confirm which tool is being used at NPCI & is tool integrated with existing SIEM & SOAR		This will be discuss with qulified bidder
213		8	Section 1 - Bid Schedule and Address	Last date and time for Bid Submission 24th July 2025, 5:00 PM	We request you to extend the date for bid submission till August 20, 2025 considering the broad scope of work and the detailing required in preparing and submitting the proposal.		Will be addressed on the NPCI website
214		12	3.1.A	Bidder should maintain a knowledge base of alerts, incidents and mitigation steps.	Is there an existing platform for knowledge base or should bidder propose one?		Existing Platform available
215		13	3.1.A	All daily routine and standard activities of L1 and L2 to be fully automated in phased manner within one year.	Please specify the list of activities to be automated and preferred automation tools.		This will be discuss with qulified bidder
216		13	3.1.A	Bidder shall perform digital forensic investigation on need basis.	Please confirm if NPCI will provide forensic tools or bidder needs to provision them.		This will be discuss with qulified bidder
217		13	3.1.A	False positive rate of the incidents has to be less than 5%.	What is the current baseline false positive rate and volume of alerts?		This will be discuss with qulified bidder
218		13	3.1.A	Bidder shall be responsible to develop and maintain SOPs and playbooks.	Are existing SOPs/playbooks available for reference or should bidder create from scratch?		SOP and playbook available
219		14	3.1.A	Bidder has to report and escalate the incidents as per the TAT defined by NPCI.	Please share the defined TAT matrix for various incident categories.		This will be discuss with qulified bidder
220		14	3.1.A	Bidder should have strong knowledge to implement/improvise existing SOAR solutions.	Please confirm the existing SOAR platform and its integration capabilities.		This will be discuss with qulified bidder
221		14	3.1.B	Bidder should conduct security trainings for NPCI nominated persons once in six months.	Please confirm the number of participants and duration of each training session.		This will be discuss with qulified bidder
222		14	3.1.B	Bidder should perform SOC Maturity assessment for multiple cycles in a year.	Please confirm the number of cycles/numbers and preferred maturity assessment		This will be discuss with qulified bidder
223		14	3.1.B	Bidder should prepare SOC operations for compliance to ISO 27001, ISO 20000, BS 25999 and PCI DSS.	Please confirm if certification is in scope or only readiness.		This will be discuss with qulified bidder
224		43	Section 9 - L2	L2 analysts to perform root cause analysis, triage incidents, and customize dashboards.	Please confirm the SIEM platform and dashboard tools to be used.		This will be discuss with qulified bidder
225		43	Section 9 - L2	Knowledge of open-source tools like ELK required.	Please confirm if ELK stack is part of the current SOC environment.		This will be discuss with qulified bidder
226		43	Section 9 - L3	L3 to perform threat modeling and define use cases.	Please confirm if existing threat models and use cases are available for reference.		This will be discuss with qulified bidder
227		32	8.12	Parser creation for unparsed events in SIEM within 1 week.	Please confirm the average number of parser creation requests expected per month.		This will be discuss with qulified bidder
228		32	8.12	Penalty of INR 10,000 per day for delay in parser creation.	Is there any grace period or exception mechanism for complex integrations?		This will be discuss with qulified bidder
229		32	8.12	Asset integration with SIEM to be completed within 3 working days.	Please confirm the average number of assets expected to be integrated monthly.		This will be discuss with qulified bidder
230		32	8.12	P1/P2 incident creation and resolution timelines for devices not reporting.	Will NPCI provide automated monitoring tools or should bidder provision them?		This will be discuss with qulified bidder
231		33	8.12	Threat Intelligence advisories to be published within 8 hours.	Will NPCI provide access to threat intel feeds or should bidder subscribe independently?		This will be discuss with qulified bidder
232		34	8.12	Architecture and solution planning timelines.	Will NPCI define the scope and frequency of such planning activities?		This will be discuss with qulified bidder
233		35	8.12	Policy & user management SLA for emergency and routine changes.	Please confirm the average number of change requests expected per month.		This will be discuss with qulified bidder

234		35	8.12	Fault management – ticket creation and updates.	Will NPCI provide access to OEM SLAs and escalation matrix?		No change in RFP
235		36	8.16	Prices shall remain fixed for 3 years with no escalation.	Please confirm if this is a no-deviation RFP or if terms can be renegotiated post selection.		No change in RFP
236		32	8.12	SLA penalties for parser creation, use case gaps, and incident response.	Please confirm if there is a cap on total SLA penalties per quarter?		No change in RFP
237		14	3.1.A	API-based integration with cloud platforms.	Please confirm the cloud platforms in scope (e.g., AWS, GCP, Azure).		This will be discuss with qulified bidder
238		59	Sr. No. 1	Management of products for fault and capacity during business hours.	Please confirm the number and types of products in scope.		This will be discuss with qulified bidder
239		60	Sr. No. 17	Backup of configuration files on change.	Please confirm the backup tool/platform in use or expected.		This will be discuss with qulified bidder
240		60	Sr. No. 23	Firewall rule base review using provided tool.	Please specify the tool to be used for firewall rule base review.		This will be discuss with qulified bidder
241		15	B. Incident Response	Resource requirement support- SOC Monitoring	NPCI to share the Years of experience for the following resources : 1. L1 2. L2 3. L3		L1 - 2 to 3 years L2 - 5 to 7 years L3 - 8 to 10 years
242		28	7.3	Technical Scoring Matrix	Please clarify if resumes of proposed resources are to be submitted at the time of bid or post award?		Yes
243		28	8.3	Technical Scoring Matrix	Please confirm if certifications like CEH, CISSP, or CompTIA CySA+ are mandatory for L1, L2, L3 roles or only preferred.		L2 and L3 its mandetory. Before onboarding NPCI will take interview of all resources.
244		28	9.3	Technical Scoring Matrix	Kindly clarify the weightage assigned to each item in the scoring matrix.		Will provide in Corrigendum 1
245		-	-	-	Please clarify the location for the deployment of the on-site resources		Hyderabad, Chennai & Mumbai
246		-	-		We have initiated internal risk and legal review process on this RFP. We request you to consider queries as and when our risk and legal team informs us about the same.		No change in RFP