Corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
1	Scope of Work and Technical Specifications	1	1.(d)	The bidder should provide all the services and tools mentioned in the RFP. There is no restriction on the number of resources to be deployed, but the bidder has to abide by the SLA.	The bidder should provide all the services and tools mentioned in the RFP. There is no restriction on the number of resources to be deployed, but the bidder has to abide by the SLA. However, resources managing the same may operate from remote locations on shared basis.
2	Scope of Work and Technical Specifications	2	(h)	The bidder will be responsible for providing deployment and 24X7X365 operational support for all the security tools proposed in this RFP, which includes, but is not limited to: Design and Architecture: Crafting the overall structure and design of the cloud infrastructure…….Security: Implementing robust physical and digital security measures to protect the system	The bidder will be responsible for providing deployment and 24X7X365 operational support for all the security tools proposed in this RFP, which includes, but is not limited to: Implementation: Realization of the design to life and ensuring all components work as intended. · Future Modifications: Updating and modifying the approved system design as and when required. · Maintenance and Support: Keeping the system in good working order and resolving any issues. · Security: Implementing robust physical and digital security measures to protect the system

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
3	Scope of Work and Technical Specifications	4	(ii)	All the tools proposed by the bidder must be in High Availability mode ensuring redundancy.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, Cloud based offering may be considered on a very special case basis subject to Data sovereignty and residency clauses. However, NABARD reserves the right to reject proposals wherein tools that are technically feasible to reside on virtual machines are offered on cloud. Additionally, all the tools deployed shall be in HA in active-active mode at all the sites.
4	Scope of Work and Technical Specifications	12	3.8.2	The EASM solution shall be seamlessly integrated with Bank's existing infrastructure devices and the proposed solution such as AD, SIEM, Firewalls, etc. The integration shall be carried out by the bidder	The EASM solution shall be seamlessly integrated with proposed SIEM solution. The integration shall be carried out by the bidder
5	Scope of Work and Technical Specifications	16	8.(d)	All review meetings will be held at NABARD's designated site.	All review meetings will be held at NABARD's designated site and mode (Physical/Virtual/Hybrid)
6	Scope of Work and Technical Specifications	17	9	Responsibility Matrix	Revised Responsibility Matrix
7	Scope of Work and Technical Specifications	23	3	The Proposed solution should have (Video) learning contents in the console itself.	Clause removed

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
8	Scope of Work and Technical Specifications	24	41	High Availability should use cluster set-up so that data could be shared between the nodes.	The setup should be in HA Mode ensuring redundancy.
9	Scope of Work and Technical Specifications	38	8	The commercial proposal should be based on FQDNs inclusive of unlimited WAF and L3-L7 DDoS (bandwidth) per FQDNS with addon options for API Security requests/month and Bot protection for transaction/month	Clause removed
10	Scope of Work and Technical Specifications	41	15	The solution should have authentication options for users/groups. It should supports authentication of users via Integrated Windows Authentication, NTLM (NTLM v1 and v2 in Session Security), and LDAP.	The solution should have authentication options for users/groups. It should support authentication of users via Directory Sync from Active Directory (AD), SAML 2.0, RADIUS, LDAP etc
11	Scope of Work and Technical Specifications	41	11	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability of detecting and blocking encrypted malicious files
12	Scope of Work and Technical Specifications	42	30	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links, etc	The proposed solution should have an ability to configure rules on web traffic coming from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links, etc.
13	Scope of Work and Technical Specifications	44	7	Automatically deploy sensor agents across DB environment using centralized implementation manager dashboard. Turn sensors on/off from single console.	Deploy sensor agents across DB environment using centralized implementation manager dashboard or

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
					with manual installation. Turn sensors on/off from single console
14	Scope of Work and Technical Specifications	44	57	The solution should support OS like VIOS, Red Hat, Ubuntu etc.	The solution should support all the OS present in the Market like Red Hat, Ubuntu , Linux, Windows etc.
15	Scope of Work and Technical Specifications	44	2	DAM Solution should provide easy & fast deployment It should be available as a predeployed virtual appliance which could be deployed on hypervisor like Nutanix, VMware etc.	DAM Solution should provide easy & fast deployment. It should be available as a software based installation which should be compatible with all the industry standard hypervisors.
16	Scope of Work and Technical Specifications	45	20	Create an audit compliance workflow for a few users allowing for comments, escalation and signoff.	Clause removed
17	Scope of Work and Technical Specifications	45	32	Define an audit review process, selecting a group of three reports and send via email for review and signoff.	Clause removed

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
18	Scope of Work and Technical Specifications	47	57 and 58	Proposed DAM solution must have proactive approach or provide visibility to advanced threats and with the ability to proactively correlate activities and give insights into the following kinds of attacks: a) SQL injection b) Malicious stored procedure c) Data leak d) Denial of service e) Account take-over f) Schema tampering g) Data tampering h) Anomaly	Proposed DAM solution must have proactive approach or provide visibility to advanced threats and with the ability give insights into the following kinds of attacks: a) SQL injection b) Malicious stored procedure c) Schema tampering d) Data tampering e) Anomalous Behaviour
19	Scope of Work and Technical Specifications	48	73	The solution should provide an internal workflow capability that allows users to raise issues and assign them to other users.	Clause removed
20	Scope of Work and Technical Specifications	63	16	The solution should be "Network Aware" and have the ability to change the client's policy based on its network location.	Clause removed
21	Scope of Work and Technical Specifications	63	26	Solution must have backups provided as part of the service Solution must be GDPR compliant	Solution must have backups provided as part of the service and should be compliant to various regulations of the Country.
22	Scope of Work and Technical Specifications	64	59	The solution will Automatically learn and authorize logged in users.	The solution will Automatically learn logged in users.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
23	Scope of Work and Technical Specifications	64	61	The solution will require that only an authorized Pre-boot user is allowed to log into Windows.	Clause removed
24	Scope of Work and Technical Specifications	64	60	Users will log on one time (SSO) for authentication to the operating system, Full Disk Encryption, and other Endpoint Security blades.	Clause removed
25	Scope of Work and Technical Specifications	65	69	The solution will be used to determine if users can connect to wireless networks while on your organization's LAN to protect the network from threats associated with wireless networks.	Clause removed
26	Scope of Work and Technical Specifications	65	70	The solution will define if users can connect to the organization network from hotspots in public places, such as hotels or airports	Clause removed
27	Scope of Work and Technical Specifications	66	102	The solution must block the user from using its corporate credentials in a site that does not belong to the corporate domain.	Clause removed
28	Scope of Work and Technical Specifications	66	104	The solution must enforce "Safe Searching" feature when they employ the Google, Bing, Yahoo or any other search engines	Clause removed
29	Scope of Work and Technical Specifications	66	97	The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content.	Clause removed
30	Scope of Work and Technical Specifications	66	103	The solution must provide URL filtering based on categories with additional Black/Whitelisting	Clause removed

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
31	Scope of Work and Technical Specifications	68	6	Network Detection and Response (NDR)/NBAD solutions take advantage of the flow technologies built into network devices. NDR /NBAD tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs data into meaningful analytics data like numbers charts and tables that quantify exactly how the network is being used, by whom and for what purpose.	Network Detection and Response (NDR)/NBAD solutions take advantage of the flow technologies built into network devices or should support full packet capture (PCAP)NDR /NBAD tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs and packet data into meaningful analytics data like numbers, charts, and tables that quantify exactly how the network is being used, by whom and for what purpose.
32	Scope of Work and Technical Specifications	68	6	Network Detection and Response (NDR)/NBAD solutions take advantage of the flow technologies built into network devices. NDR /NBAD tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs data into meaningful analytics data like numbers charts and tables that quantify exactly how the network is being used, by whom and for what purpose.	Network Detection and Response (NDR)/NBAD solutions should take advantage of either the flow technologies built into network devices or full packet capture (PCAP). NDR /NBAD tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs and data into meaningful analytics data like numbers, charts, and tables that quantify exactly how the network is being used, by whom and for what purpose.
33	Scope of Work and Technical Specifications	68	9	NDR/NBAD solution should be able to use the existing network environment as a sensor grid to analyse traffic flow across the across the existing network and security solutions in a non-disruptive manner	NDR/NBAD solution should be able to use the existing network environment as a sensor grid to analyse traffic flow or packets

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
					across the existing network and security solutions in a non-disruptive manner
34	Scope of Work and Technical Specifications	68	2	The NDR/NBAD tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NDR/NBAD integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.	The NDR/NBAD tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NDR/NBAD integrates user /hostname information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.
35	Scope of Work and Technical Specifications	68	3	The NDR /NBAD solution should also offer the flexibility and capability to drill down into the end user, MAC, flows, interface utilization and a wide array of other host statistics needed for rapid incident resolution. Should utilize anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration. The Solution should be able to detect Malwares on both encrypted and nonencrypted payloads.	The NDR /NBAD solution should also offer the flexibility and capability to drill down into the end user or hostname or MAC, flows or packet, interface or application or server or host utilization and a wide array of other host statistics needed for rapid incident resolution. Should utilize anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration. The Solution should be able to detect Malwares on both encrypted and nonencrypted payloads.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
36	Scope of Work and Technical Specifications	69	17	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.	The solution should support all forms of standard flow formats including but not limited to NetFlow, IPFIX, sFlow, Jflow or support Full Packet Capture (PCAP).
37	Scope of Work and Technical Specifications	69	10	The solution should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.	The solution should allow discovery function to identify/add network devices and capture information such as IP address, OS, services provided, other connected hosts.
38	Scope of Work and Technical Specifications	69	13	The system should be able to monitor flow data between various VLANs.	The system should be able to monitor flow or packet data between various VLANs.
39	Scope of Work and Technical Specifications	69	18	The solution should be able to combine/stitch the flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation and present them as a single bi-directional flow record.	The solution should be able to combine/stitch/capture the flow records/network packets coming from different network devices like routers, switches, firewalls that are associated with a single conversation and present them as a single bi-directional flow record.
40	Scope of Work and Technical Specifications	69	19	The solution must be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.	The solution must be able to stitch flows/capture packets into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
41	Scope of Work and Technical Specifications	70	45	The solution should perform analysis on network data all the way up to the Layer 7 and provide complete application visibility	The proposed NDR/NBAD solution must support deep traffic analysis to ensure complete application-level visibility. The solution should be capable of analyzing either flow-based or packet-based data and must offer flexibility in deployment based on the organization's network architecture. The bidder may propose either a NetFlow-based or packet-based NBAD solution, provided it meets the requirement for comprehensive visibility and threat detection across the full stack.
42	Scope of Work and Technical Specifications	71	63	NDR/NBAD solution should provide a full-featured Network threat analyser capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.	NDR/NBAD solution should provide a full-featured Network threat analyser capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow or packet analysis techniques and the ability to detect deviations from normal baselines.
43	Scope of Work and Technical Specifications	72	68	The solution must be able to provide visibility of user endpoint workstations and support & service options to collect telemetry from these endpoints including username, process names and process hashes involved in the network traffic. If there is any License to be provided, the same should be considered for 50 endpoint	Clause removed

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
				workstations from day one.	
44	Scope of Work and Technical Specifications	73	100	The solution should allow taking logs from proxy and enrich that to flows for showing users behind the proxies.	The solution should allow taking logs from proxy and enrich that to flows /PCAP for showing users behind the proxies.
45	Scope of Work and Technical Specifications	73	99	The solution should have an automated scanner to identify assets and should also be able to schedule the scans	The solution should have capability to identify assets and correlate the network behaviour.
46	Scope of Work and Technical Specifications	74	103	The solution should have native integration with any PDNS service to obtain unlimited DNS resolution and domains hosted information along with WHOIS directly from the portal	Clause removed
47	Scope of Work and Technical Specifications	74	105	The solution should have native integration with CERT CMTX & NCIIPC Threat Feeds	The solution should support ingestion of threat feeds from CERT CMTX, NCIIPC or any other regulatory requirement via global standard methods.
48	Scope of Work and Technical Specifications	77	54	The platform should be able to provide the details of internet-facing assets with Visualization graphs to cover below scope: 1. Discovered root domains 2. Hosts 3. Ips 4. Assets by location	Clause removed

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
				5. Domain's discovery trends over the period of last 12 months	
49	BOM and Commercials				Revised Commercial Format
50	Minimum Eligibility Criteria	2	7	**Experience** a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for at least 3 distinct clients in the last 5 years (FY 2024-25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches. (This shall override experience criteria given in the bid in other documents)	**Experience** a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for at least 3 distinct clients in the last 5 years (FY 2024-25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Bank in India having more than 500 branches. (This shall override experience criteria given in the bid in other documents)

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
51	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, at least 50 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/OSCP/ CEH certified. Note: (i) Resources for CEH Max 10 resources shall be considered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource is carrying more than one certification, it shall be considered as one.	The Bidder shall have minimum 50 security professionals supporting security and SOC solutions in India on bidder's payroll in/any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, at least 25 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/OSCP certified. Note: (i) If a resource is carrying more than one certification, it shall be considered as one. The certification date must be prior to the date of publication of this RFP. (ii)The certificates provided by the bidder for the resources should be valid at the time of publishing of bid. The resource should on bidder's payroll before publishing of bid. A list of resources mentioning the employee

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
					Number , Employee name, and date of appointment to be provided.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
52	Payment Terms and Conditions	1	3	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 10% cost of the monthly contracted amount. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the monthly contracted amount even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 10% cost of the monthly contracted amount. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the monthly contracted amount even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor. The overall penalty shall not exceed 25% cost of the monthly contracted amount.
53	QCBS Evaluation Criteria	4	C	Scoring Criteria for bidder Certifications: a. ISO27001 Certification - 2 Marks b. Cert-in Empanelment - 2 Marks c. SOC II Type II Certification - 1 Marks All these certifications should be valid as on 1st April 2025.	Scoring Criteria for bidder Certifications: a. ISO27001 Certification - 2 Marks b. Cert-in Empanelment - 2 Marks c. SOC II Type II Certification - 1 Marks All these certifications should be valid as on the date of submission of Bid.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
54	QCBS Evaluation Criteria	4	D	The bidder must have IT Security resources on permanent payroll having experience in-scope solutions with Certifications such as CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) 50 to 75 resources- 04 marks (b) 76 and above resources- 09 marks Note: (i) Resources for CEH- Max 10 resources will be considered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource has more than one certification, it will be considered as one. (iii) Of the above, the bidder must have a total of 5 certified resources of the proposed SIEM solution on permanent payroll. If not, then the count of resources will not be considered, and no marks shall be awarded under Clause 'D'.	The bidder must have IT Security resources on permanent payroll having the Certifications such as CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ECSA/ CREST/ CISM/ CISA/ OSCP (a) 25 to 50 resources- 04 marks (b) 51 and above resources- 09 marks Note: (i) The certification date must be prior to the date of publication of this RFP. (ii) If a resource has more than one certification, it will be considered as one. (iii) Of the above, the bidder must have a total of 5 certified resources of the proposed SIEM solution on permanent payroll. If not, then the count of resources will not be considered, and no marks shall be awarded under Clause 'D'. (iv) Bidder has to submit a declaration regarding the same on its letterhead clearly complying with all the conditions mentioned above. (v)The certificates provided by the bidder for the resources should be valid at the time of publishing of bid. The resource should on bidder's payroll before publishing of bid. A list of resources mentioning the employee

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
					Number , Employee name, and date of appointment to be provided.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
55	QCBS Evaluation Criteria	4	B.2.(A) - B.2.(J)	(A) The proposed SIEM solution with a minimum of 10000 EPS should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 7 marks (b) 13 to 14 references -5 marks.....OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices/signoff Letter	(A) The proposed SIEM solution with a minimum of 10000 EPS should be implemented in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Reference: (a) 15 references and above- 7 marks (b) 13 to 14 references -5 marks (c) 10 to 12 references- 3 marks (B) The proposed SOAR + TIP solution should be implemented in India in last five years (FY2020-2021, FY2021-2022, FY2022-2023, FY2023-2024, FY 2024-2025): Reference: (a) 10 references and above- 4 marks (b) 08 to 09 references -3 marks (c) 05 to 07 references- 2 marks (C) The proposed WAF solution should be implemented in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023- 2024, FY 2024-2025): Reference:

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
					(a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (D) The proposed DAM solution should be implemented in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Reference: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (E) The proposed SWG solution should be implemented in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023- 2024, FY 2024-2025): Reference: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (F) The proposed PAM solution should be implemented in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025):

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
					Reference: (a) 10 references and above- 4 marks (b) 08 to 09 references -3 marks (c) 05 to 07 references- 2 marks (G) The proposed EDR solution with should be implemented in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Reference: (a) 10 references and above- 4 marks (b) 08 to 09 references -3 marks (c) 05 to 07 references- 2 marks (H) The proposed EASM solution should be implemented in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Reference: (a) 10 references and above- 3 marks (b) 08 to 09 references -2 marks (c) 05 to 07 references- 1 marks (I) The proposed SCM solution should be implemented India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023,

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
					FY 2023- 2024, FY 2024-2025): Reference: (a) 10 references and above- 3 marks (b) 08 to 09 references -2 marks (c) 05 to 07 references- 1 marks (J) The proposed NBAD solution should be implemented in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023- 2024, FY 2024-2025): Reference: (a) 10 references and above- 4 marks (b) 08 to 09 references -3 marks (c) 05 to 07 references- 2 marks All OEMs shall submit a declaration on their official letterhead confirming the details of the client organization where the proposed solution has been implemented. The declaration must include the name of the solution, implementation start and end dates, and the current validity status of the solution in the client environment

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
56	Service Level Agreement	18	18.1	Service Provider liability to meet the SLAs is limited to 10% cost of agreement during the period of the contract in which the liability event occurred. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the payments even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor.	Service Provider liability to meet the SLAs is limited to 10% cost of agreement during the period of the contract in which the liability event occurred. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the payments even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor. The overall penalty shall not exceed 25% cost of the contracted amount.
57	Service Level Agreement	28	28.2	If the Service Provider fails to deliver any Support Services or meet any Service Levels under this Agreement, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' subject to maximum of 10% cost of the underperformed services. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the payments even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor.	If the Service Provider fails to deliver any Support Services or meet any Service Levels under this Agreement, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' subject to maximum of 10% cost of the underperformed services. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the payments even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Modified Clause
					The overall penalty shall not exceed 25% cost of the monthly contracted amount.
58	Service Level Agreement	24	23.2.h	If the SLA penalties/Liquidated damages during the operations phase (Post Go-Live) calculations equals or exceed 10% of the billing for six consecutive months	If the SLA penalties/Liquidated damages during the operations phase (Post Go-Live) calculations equals or exceed 10% of the billing for three consecutive months
59	Scope of Work and Technical Specifications			Additional Clause	The bidder has to ensure 99.999 availability of its DC and DR. and ensure adequate BCP processes are in place.
All the changes carried out through Corrigendum in the RFP shall correspondingly reflect in the SLA while signing with the successful bidder					

Responses to Prebid Queries

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
1	Minimum Eligibility Criteria	2	7	**Experience** a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024-25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches. (This shall override experience criteria given in the bid in other documents)	We have multiple contracts with same client, we request NABARD to consider the same as for qualification.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
2	Service Level Agreement	23	23	Termination	There are no rights of termination to the bidder, we request this to be mutual as there are some specific scenarios where the bidder needs the right for termination with prior approval for NABARD	No change
3	General			Additional Point	Who will provide hardware, since the hosting is in Ctrls, we assume NABARD will provide the hardware for hosting the cyber security solution	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
4	General			Additional Point	We understand NABARD has recently signed a contract with CTRLS , however since the infra is hosted at ctrls there might be a scenario that the bidder might need products / services from ctrl s, hence we request NABARD to allow the bidder to outsource some of the above products / solution / services to ctrls, however the bidder will take entire ownership of the solution and will abide all the SLA's.	The same is not allowed.

5	Scope of Work and Technical Specifications	4	hh	Technical Specifications of all the tools mentioned below are detailed in the Technical Specification Sheet. At the end of the implementation, the bidder has to arrange for a Certificate from the respective OEMs, certifying that the implementation deployed solution meets all the technical/functional specifications of the solution as specified in Technical Specifications in this RFP.	1. We understand NABARD needs entire solution on opex , however certain solutions like DAM are not available on MSSP / OPEX model by the OEM hence we request NABARD to allow bidders to charge one time supply and implementation in addition to OPEX charges, as above solutions are not available on OPEX or NABARD cannot terminate the contract for 3 years. 2. Since NABARD has recently signed a contract with CTRL S we assume hardware will be provisioned by NABARD at no cost to the bidder. 3. as per RFP NABARD has not asked for DDoS Solution , then how can this be in bidder scope, we request you to pls delete this clause, also the network in not in bidders scope 4. Dedicated/ Shared model – Since the security components will have access to the network, we need NABARD to confirm if the services can be given on shared model.	1. All the tools provisioned as part of the RFP shall be provided on a dedicated basis. However, Resources managing the same may operate remotely in sharing mode. 2. NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites. 3.DDoS Solution is not in the bidder's scope. However, Bidder has to configure all the proposed security solutions to prevent DOS and DDOS attacks on NABARD infra.

						4. All the tools provisioned as part of the RFP shall be provided on a dedicated basis. However, Resources managing the same may operate remotely in sharing mode.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
6	BOM and Commercials	1			is NABARD referring to reduce the minimum commitment given in the commercial bid, even if NABARD does not consume minimum commitment , still NABARD will pay for minimum commitment	Irrespective of the load, NABARD will pay for minimum for minimum commitment. However, any load over and above the minimum commitment shall be charged on pay per use basis.
7	Scope of Work and Technical Specifications	1	1.(b)	The solution will be procured on an operational expenditure (Opex) basis, ensuring high availability and allowing for a rate contract to accommodate any additional or enhanced requirements as they arise	Service Provisioning Locations: as there will be some or the other services given out of cloud/Internet, does NABARD need 3 same provisioning sites or can be managed out of anywhere within India Meity Certificated DC/Cloud.	Bidder to propose HA in in all locations sites.
8	Scope of Work and Technical Specifications	2	(g)	The Managed Services for NABARD should include a comprehensive suite of IT management and monitoring activities. These services should cover:	do we need to integrate with existing IT management & monitoring solution, we will not provide another monitoring solution as this can be done on individual solution console	In addition to the monitoring tools provided by the bidder, the tools shall be integrated with the tools provided by NABARD.
9	Scope of Work and Technical Specifications	2	(g)	Online Portal: Integrating into the existing portal provided by the Bank for availability and performance	Pls share the online portal details for integration, what is the purpose of this integration	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				reporting which should be monitored on 24/7 basis.		
10	Scope of Work and Technical Specifications	3	(m)	The entire solution shall be scalable at short notice within 1 month of the request from NABARD and shall be governed by SLA	there are some solutions that needs time for integration hence pls amend this to 3 months	No change
11	Scope of Work and Technical Specifications	3	(w)	All tools supplied as part of the project should undergo annual health checkup by the respective OEMs and the certificate for same should be submitted to NABARD.	Since these solutions are provided in MSSP from bidders / NABARD setup , OEM cannot certify these solution , this is only possible if you have a dedicated setup in shared setup other clients data is also there hence OEM cannot look into all the clients data	Bidder has to provide the tools in a dedicated manner. However, the resources managing the same can be on shared basis.
12	Scope of Work and Technical Specifications	4	(hh)	Technical Specifications of all the tools mentioned below are detailed in the Technical Specification Sheet. At the end of the implementation, the bidder has to arrange for a Certificate from the respective OEMs, certifying that the implementation deployed solution meets all the technical/functional specifications	Since these solutions are provided in MSSP from bidders / NABARD setup , OEM cannot certify these solution , this is only possible if you have a dedicated setup in shared setup other clients data is also there hence OEM cannot look into all the clients data	All the tools provisioned as part of the RFP shall be provided on a dedicated basis. However, Resources managing the same may operte remotely in sharing mode.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				of the solution as specified in Technical Specifications in this RFP.		
13	Scope of Work and Technical Specifications	4	(ii)	All the tools proposed by the bidder must be in High Availability mode ensuring redundancy.	We assume the hardware will be provided by NABARD in HA mode	Kindly refer to corrigendum
14	Scope of Work and Technical Specifications	5	(mm)	All the tools proposed as part of the RFP shall be integrated with the existing infrastructure of the Bank, ensuring seamless integration of all the solutions among themselves.	Assuming these tools will have the required API for integration with relevant use cases	All the tools have API based integration facility

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
15	Scope of Work and Technical Specifications	5	(nn)	The Solution deployed as part of the RfP shall not be extended to any 3rd party.	Since this is a MSSP setup , our licenses for SIEM etc will be shared with other clients, if you want a dedicate setup then you need to consider one time fee	All the tools provisioned as part of the RFP shall be provided on a dedicated basis. However, Resources managing the same may operate remotely in sharing mode. Payment will be made as per the payment mentioned in the RFP
16	Scope of Work and Technical Specifications	5	3.1	SIEM with SOC services	Pls share the entire list of all the assets / applicationt to be integrated with the SIEM, this will have an impact on our commercials hence we need the list for integration	Same shall be shared with the successful bidder.
17	Scope of Work and Technical Specifications	5	3.1.4	Installation and commissioning of adequate log collector at Bank sites (DC, DR and Near Site). Ensure that logs are being collected from all the in-scope devices. As appropriate suggest Bank and related stakeholders on required log-levels and support Bank in enabling the suggested log levels	Does NABARD need all the MSSP mentioned solutions installed in HA in all the 3 sites , for eg you can install only collectors in other 2 sites and just keep the console in DC, this will optimise the cost	Bidder has to provide all the solution in HA mode under active active at all sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
18	Scope of Work and Technical Specifications	6	3.2.1	The MSSP Bidder shall be responsible for supply, implementation, maintenance and support of SOAR Solution at Bank's infrastructure.	as per this clause , is NABARD looking for a dedicated SOAR tool at banks infras , or else we can do this in MSSP where we can use our shared licenses, a dedicated tool and setup will increase the cost, and will also need one time setup fee in case you are looking for dedicated SOAR solution	All the tools provisioned as part of the RFP shall be provided on a dedicated basis. However, Resources managing the same may operate remotely in sharing mode.
19	Scope of Work and Technical Specifications	6	3.2.7	The Solution (with each of its components) should be configured in High Availability (HA) mode.	the solution is hosted in our environment in HA , since we will be using our MSSP setup we will use our existing config	All the tools provisioned as part of the RFP shall be provided on a dedicated basis. However, Resources managing the same may operate remotely in sharing mode.
20	Scope of Work and Technical Specifications	12	3.8.2	The EASM solution shall be seamlessly integrated with Bank's existing infrastructure devices and the proposed solution such as AD, SIEM, Firewalls, etc. The integration shall be carried out by the bidder	EASM is an independent SaaS solution, this need not be integrated with AD, Firewalls, etc , hence pls remove this clause	Please refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
21	Scope of Work and Technical Specifications	15	4.(a)	The bidder shall arrange an annual health check of all the proposed security solutions by OEM. The coordination with OEM for completion of Health checks is Bidders responsibility. All costs associated with the audit/Health check shall be borne by the bidder. Bidder has to submit an independent Health check report for all security solutions with NABARD. The health check shall cover the following things but not limited to:	Since this is MSSP setup, OEM cannot individually verify the solution as this will be shared amongst multiple clients	Please refer to the RFP
22	Scope of Work and Technical Specifications	15	4.(b)	Bidder shall also allow NABARD to Audit/review the setup remotely and/or On Site by its own team and/or by any 3rd party Auditor appointed by NABARD on regular basis	Since this is a MSSP / Shared setup the audit review will be limited to NABARD infra only	Kindly refer to the RFP
23	Scope of Work and Technical Specifications	15	5.(a)	Complaince - Isolation of NABARD's digital and physical data path from other clients.	This is a shared setup , diff physical and digital path will not be possible	The bidder has to deploy all the tools in a dedicated manner for the Bank. However, resources managing the same may provide the services remotely in a shared mode.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
24	Scope of Work and Technical Specifications	16	6.(c)	Training shall be provided by the OEM certified Trainers only.	Training will be provided by OEM certified resources on bidders payroll	No Change
25	Payment Terms and Conditions	1	1 and 2	Invoices shall be generated on monthly basis, reflecting the SLA levels for that month, and will include any applicable penalties. Payment shall be made on a quarterly basis, in arrears	We assume billing and payment both should be qtrly	Kindly refer to the RfP
26	Payment Terms and Conditions			Additional Point	Since some solutions will be bought dedicatedly for NABARD like DAM, NBAD, etc we would request NABARD to pay one time fee for supply and implementation as it was required one time investments or if NABARD wants us to divide the entire investment over 5 years for fixed price, in case NABARD terminates the contract in between then	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					NABARD to pay the residual value	
27	Payment Terms and Conditions	1	3	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 10% cost of the monthly contracted amount. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the monthly contracted amount even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate	The overall LD is not capped, hence we request NABARD to cap the max LD to be 10% of the monthly price	Please refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				payment for the downtime except for approved downtime shall not be made to the vendor		
28	Project Timelines and Deliverables	1		Installation, configuration and commissioning of the tools	Since some of the solutions will be bought dedicatedly for NABARD we will need 3 months for supply , delivery and implementation	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
29	QCBS Evaluation Criteria	2	B.1	Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22, 2020-21 (Bidder shall submit PO/credential letters)	we request you to delete "minimum of 4 solutions" , also pls change 10K EPS to 5K EPS , and remove SOAR as well, as many clients have not opted for SOAR solution hope we can submit global references here.	No Change
30	Service Level Agreement	15	16	Confidentiality	Overall confidentiality clause is a bit open / generic will need revision at the time of contracting and shall survive for a period of 1 year post termination of the engagement.	No change
31	Service Level Agreement				The terms in SLA needs revision as this will be a MSSP contract and some solution will be on shared model	No change
32	Service Level Agreement	18	18	Limitation of Liability	Liability should be max capped to the yearly contract value	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
33	Service Level Agreement	28	28	Liquidated Damages	1. Overall Penalty & LD is uncapped, we request you to accept 10% overall LD of monthly invoice 2. Indirect and consequential damages should be capped to max yearly contract value 3. We request NABARD to provide indemnity for third party claims to the bidder	No Change
34	Non-Disclosure Agreement	4	Annexure II		Permitted Disclosure: The Disclosing Party agrees that if the Confidential Information is required to be disclosed pursuant to any order or requirement from court, administrative or governmental agency, such Confidential Information can be disclosed, provided the Receiving Party gives, if legally permitted, the Disclosing Party a prompt written notice of such order or requirement and an opportunity to contest or seek an appropriate protective order under law.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					Retention: The Bidder may retain copies of such Confidential Information reasonably required to be retained in accordance with law, regulation, professional standards and standard archival processes.	
35	General			Additional Point	All the Deliverables / reports , etc submitted by the bidder are for internal use and cannot be shared with any third party without prior written consent of the Bidder.	Kindly refer to the RFP
36	General			Additional Point	while submitting the response bidder will submit the sytems testing agreement and EULA for NABARD acceptance, this has to be as per OEM policy	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
37	Service Level Agreement	10	6	Audit Services	Since this is a shared setup, in no event shall any access be provided to, Bidder's networks or systems or premises or restricted areas in premises. Except where audit is required by a regulator, if a third party is conducting an audit, it shall be mutually agreed third party and prior notice of 30 days would be provided. The third-party auditor of Bank shall be mutually agreed, such agreement not unreasonably withheld. This right shall be for the term of the Contract and one year thereafter. All results of audit shall be kept confidential. Bidder shall only be liable to provide soft copies of time and expense sheet for audit.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
38	Service Level Agreement	18	18	Limitation of Liability	Bidder's aggregate liability shall be limited to the total fees paid to the bidder in the preceding 12 months for the services under the purchase order/work order which gave rise to the claim. In no event shall the Bidder be liable for any indirect or consequential losses. Accordingly, the reference to total contract value shall mean the value of the PO and services which gave rise to the claim. Bidder shall be only responsible and liable as per terms herein for the services provided by it (services exclude products/solutions provided by the OEM). OEM (and not the Bidders) shall be responsible and liable for any Products provided by it subject to its end user terms/EULA	No Change
39	Service Level Agreement	22	22	Indemnification	indemnities mentioned in the RFP are very wide and ET to disapply these indemnities and/or seek restrict indemnity only for third party claims	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					related to breach of IPR arising out of use of deliverables provided by Bidder	
40	Scope of Work and Technical Specifications	15	5	Compliance	Bidder shall comply on with applicable laws, local conditions, regulatory and statutory guidelines only to the extent they are applicable on the Bidder	Kindly refer to the RFP
41	General			Additional Point	We request NABARD to extend the bid til 20th August 2025	No change
42	Minimum Eligibility Criteria	2	7	Experience	We request you to pls accept RBI / SEBI / MCX / IRDAI as a reference	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
43	QCBS Evaluation Criteria	2	B.2.(A) - (J)	(A) The proposed SIEM solution with a minimum of 10000 EPS should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 7 marks (b) 13 to 14 references -5 marks.....OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices/signoff Letter	1. OEM will not have end client PO as they get PO from Disti / Partner, request you to pls accept that, also OEM does not do the implementation they only supply hence the PO will only be for supply 2. Also for OEM reference where they need to provide 15 reference they will submit PO copy of cloud / on prim / hybrid setup of the proposed solution as clients use same software in different form	Kindly refer to corrigendum
44	General			Additional Point	VPN connectivity to our shared setup will be provided by NABARD	Yes

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
45	General			Additional Point	as discussed in the prebid meeting will SaaS solution get an advantage over physical box solution	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
46	Service Level Agreement	10	7.2	The Service Provider shall appoint sufficient number of individuals in order to ensure that the Support Services are provided to NABARD in a proper, timely and efficient manner. The Service Provider shall provide NABARD with the names of the individuals who shall be involved in carrying out the Support Services and shall obtain approval in writing from NABARD before making any change in such team. The individuals appointed by the Service Provider shall be those indicated by the Service Provider under its response to the RFP/GeM Bid. Any additional individual shall be appointed subject to prior written approval from NABARD	as per pre bid discussion, resources can be shared however this clause is asking for dedicated and named resources, since the services will be provided from shared soc environment dedicated named resources will not be possible.	All the tools provisioned as part of the RFP shall be provided on a dedicated basis. However, Resources managing the same may operate remotely in sharing mode.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
47	Service Level Agreement	11	7.4	The Service Provider shall maintain electronic books of accounts, log-books and any other operating records that it may deem necessary in connection with the rendering of Support Services under this Agreement. The Service Provider shall retain all such electronic books of accounts and operating records relating to the Support Services for a period of 7 (seven) years after the expiry or earlier termination of the Agreement.	Since this is a dedicated setup and all the logs will be in NABARD environment we cannot copy the logs and retain a copy of it, we request you to pls delete the clause	No change
48	Service Level Agreement	11	7.6	Upon receipt of advance notice of 3 (three) Business Days from NABARD, whether during the Term or thereafter, the Service Provider shall permit NABARD and/or its Authorized Representative(s) to, during normal business hours on any Business Day, access its premises to inspect the electronic records maintained by the Service Provider in relation to the Project.	Upon receipt of advance notice of 3 (three) Business Days from NABARD, whether during the Term or thereafter, the Service Provider shall permit NABARD and/or its Authorized Representative(s) to, during normal business hours on any Business Day, access its premises to inspect the electronic records maintained by the Service Provider in relation to the Project.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
49	Service Level Agreement	37	3.1	SLAs for Security Solutions viz. SIEM, SOAR, WAF, DAM, SWG, PAM, EDR, EASM, TIP, SCM, NBAD on individual basis		No change
50	Service Level Agreement	37	3.1	Uptime = {1 – [(IT Infrastructure /Devices/Tools downtime)/ (Total Time –Maintenance Time)]}	Since the infra will be provided by NABARD the uptime calculation needs to be revised and only software related downtime be applicable to the bidder	Kindly refer to the RFP
51	Service Level Agreement	38	3.1	During the contract of the project NABARD in consultation with bidder can enforce the improvement of the SLA from 99.982% to higher value. The bidder shall ensure that there shall never be a single instance where the Security Setup is down for more than 15 mintes in a single stretch.	Since the hardware is provided by NABARD , penalties to be charged only for the reasons attributable to bidder, also any changes in the SLA should be mutually discussed with the bidder	Kindly refer to the RFP
52	Service Level Agreement	38	3.2	SLAs for Support Operations for Security Solutions	The bidder can resolve only the incidents in bidders preview , in case the incidence is for Server / Hardware / networking / virtualization, etc that is not in bidders scope those penalties will not be applicable to the bidder	All the penalties pertaining to the MSSP shall be applicable on the tools provided by them

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
53	Service Level Agreement	39	3.3.1	SLAs for updates and upgrades BIDDER shall upgrade the system/firmware of all applicable systems such as security components and tools, storage systems and any other applicable device or tool and such upgrade shall be limited to n-1 version where n is the latest version	pls ammend this to n-1 version, within 30 days	No change
54	Service Level Agreement	40	3.3.4	Vulnerability assessment and Penetration Testing Closure	All the solutions that are in bidders scope only	Closure of the VAPT recommendations is in bidders.
55	Service Level Agreement	41	3.5	SLAs for Service Desk	Since the service desk is provisioned by NABARD / Ctrls this might not be applicable to bidder	Service Desk is a ticketing tool where all the tasks will be assigned to MSSP. Bidder to abide with the SLAs.
56	Service Level Agreement	42	3.6	SLAs for Incidence Response	This is only applicable for solutions in bidders scope	Please refer to the RFP
57	Service Level Agreement	43	3	NABARD can prescribe specific periods when the system should be available 100% and if the system does not meet SLA, 2x SLA penalties will be charged for that month in which the system does	Pls clarify what specific periods you are ref to, also the hardware is provided by NABARD hence this is only applicable to the scope provided by the bidder. Pls cap the overall penalty to	Same shall be shared with the successful bidder

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				not meet the SLAs for the prescribed period.	10% on the monthly invoice value	
58	General			Additional Point	We request NABARD to pls cap the liability to a maximum of the contract value	Please refer to the RFP
124	Scope of Work and Technical Specifications	65	62	The solution should provide management of all endpoint ports, with centralized logging of port activity for auditing and compliance.	Request for Clause Removal: The given specification is not relevant to Endpoint, EDR, or Device Control. Additionally, most EDR vendors do not provide visibility into port numbers, as this is typically managed at the endpoint or network level. Therefore, we kindly request the removal of this clause from the compliance requirements.	No change
125	Scope of Work and Technical Specifications	65	65	The solution will enforce required Applications and Files based on the compliance settings by monitoring for the presence of specified files, registry values, and processes that	Request to modify clause as Solution will allow only whitelisted applications on the endpoint. Allother applications will be blocked by default	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				must be running or present on endpoint computers.	without any modofication to the policy	
61	Scope of Work and Technical Specifications	66	97	The solution must have scrubbing capabilities with no added hardware. Incoming files will be extracted of all potential malicious content such as scripts, macros and active content.	Request NABARD to modify the caluse to the below: "The solution must provide advanced malware analysis and inline threat prevention for active content in files, without requiring additional hardware" Justification: Cortex XDR provides advanced file inspection and threat detection, but scrubbing is outside the standard scope of an XDR platform. Typically this is the scope of email/file gateway or advanced threat protection tools	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
62	Scope of Work and Technical Specifications	66	98	When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	Request NABARD to remove the caluse Justification: Cortex XDR provides advanced file inspection and threat detection, but scrubbing is outside the standard scope of an XDR platform. Typically this is the scope of email/file gateway or advanced threat protection tools	Kindly refer to corrigendum
63	Scope of Work and Technical Specifications	63	16	The solution should be "Network Aware" and have the ability to change the client's policy based on its network location.	Request NABARD to remove the caluse: Justification: This clause is favouring a single OEM and removal of this clause will allow other OEMs to participate Ideally the organisations demand for the protection policies to remain the same irrespective location of the user. We recommend NABARD to not implement loose policies when the users are in the internal network and tight/strict policies when the users are out of the internal network	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
64	Scope of Work and Technical Specifications	64	59	The solution will Automatically learn and authorize logged in users.	Request NABARD to modify the caluse to the below: "The solution will Automatically learn logged in users." Justification: Authorisation is not relevant to XDR/EDR as a solution this caluse requires ideally a NAC to control the authorisation of rogue device	Kindly refer to corrigendum
65	Scope of Work and Technical Specifications	64	60	Users will log on one time (SSO) for authentication to the operating system, Full Disk Encryption, and other Endpoint Security blades.	Request NABARD to remove the clause: Justification: XDR operates at the post-boot, post-login stage, and identity management and encryption tools control pre-boot/SSO behavior. This functionality is typically provided by identity providers (e.g., Azure AD, Okta) and endpoint management tools (e.g., Intune, BitLocker), not by endpoint detection and response (EDR/XDR)	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
66	Scope of Work and Technical Specifications	64	61	The solution will require that only an authorized Pre-boot user is allowed to log into Windows.	Request NABARD to remove the clause: Justification: Pre-Boot Authentication is outside its functional scope. You need a Full Disk Encryption (FDE) product with PBA for this requirement.	No change
67	Scope of Work and Technical Specifications	66	101	The solution must block the user from browsing to a known malicious URLs or domains.	Request NABARD to remove the clause: Justification: URL filtering and DNS-layer enforcement are best achieved via SASE/NGFW solutions and is not in the scope of EDR/XDR	No Change
68	Scope of Work and Technical Specifications	66	102	The solution must block the user from using its corporate credentials in a site that does not belong to the corporate domain.	Request NABARD to remove this clause Justification: XDR cannot monitor or block the use of corporate credentials on non-corporate websites. This is a native function of DLP, CASB, or browser security platforms.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
69	Scope of Work and Technical Specifications	66	103	The solution must provide URL filtering based on categories with additional Black/Whitelisting	Request NABARD to remove this clause Justification: XDR cannot monitor or block the use of corporate credentials on non-corporate websites. This is a native function of DLP, CASB, or browser security platforms.	Kindly refer to corrigendum
70	Scope of Work and Technical Specifications	66	104	The solution must enforce "Safe Searching" feature when they employ the Google, Bing, Yahoo or any other search engines	Request NABARD to remove this clause Justification: XDR cannot monitor or block the use of corporate credentials on non-corporate websites. This is a native function of DLP, CASB, or browser security platforms.	Kindly refer to corrigendum
71	Scope of Work and Technical Specifications	66	105	The user must not be able to remove the browsing protection in any way	Request NABARD to remove this clause Justification: Browser protection is not a function of EDR/XDR	No Change
72	General			Additional Point	Request NABARD to confirm the number of endpoints	Please refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
73	Scope of Work and Technical Specifications	40	7	The solution should provide at least below mentioned security categories right from first day: 1) Advanced Malware Command and Control Category 2) Advanced Malware Payload Detection Category 3) Malicious embedded links and iframe detection category 4) Mobile Malware Category 5) Key logger and Spyware category 6) P2P software database from day 1 to control/block the below P2P protocols.	Request NABARD to remove the below categories: 4) Mobile Malware Category 5) Key logger and Spyware category Justification: The above categories are a part of Antivirus and AntiSpware engines which will cater the requirement of NABARD, hence the requirement of the above within URL categories is not necassary unless this RFP is favouring any specific OEM. In order to neutralise the rfp request you to remove the above.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
74	Scope of Work and Technical Specifications	41	11	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.	Request NABARD to modify the clasue to the below: "The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability of blocking password protected files and unknown encrypted malicious files" Justification: No security solution can decrypt and analyze password-protected content without the password unless brute-forced or guessed (which is impractical in real-time), however many OEMs take the standard and best-practice approach by blocking or flagging such files	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
75	Scope of Work and Technical Specifications	41	15	The solution should have authentication options for users/groups. It should supports authentication of users via Integrated Windows Authentication, NTLM (NTLM v1 and v2 in Session Security), and LDAP.	Request NABARD to change the clause as below: "The solution should have authentication options for users/groups. It should supports authentication of users via Directory Sync from Active Directory (AD), SAML 2.0, RADIUS, LDAP" NTLM and Integrated Windows Authentication is generally considered outdated and less secure. Palo Alto recommends modern SAML/OAuth/Kerberos-based mechanisms.	Kindly refer to corrigendum
76	Scope of Work and Technical Specifications	42	20	The solution should support configuring scheduled automatic backup of system configuration.	Request to change clause as follows: The Cloud Native Platform must be resilient to have backup of tenant configurations and have High Availability and Disaster Recovery sites at Management Plane level.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
77	Scope of Work and Technical Specifications	42	27	The solution should create custom reports on a granular and/or enterprise level. The solution should have capabilities to automatically deliver reports based on schedule to selected recipients.	Request NABARD to change the clause as below: "The solution should offer comprehensive, pre-defined reports that are rich in detail and cover a wide range of security, user activity, and traffic insights. These reports can be automatically delivered to selected recipients on a scheduled basis. Custom reporting is not required, as the extensive set of built-in reports fully meets the needs for both granular and enterprise-level analysis, ensuring simplicity and efficiency without the need for complex customization."	No change
78	Scope of Work and Technical Specifications	42	30	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links, etc	Request NABARD to remove this clause: Justification: This clause is a requirement of an NMS tool and does not fall under the scope of a SWG requirement	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
79	Scope of Work and Technical Specifications	43	40	The solution should be capable of managing cross-domain requests.	Request NABARD to help with a more detailed understanding of this requirement	Kindly refer to the RFP
80	Scope of Work and Technical Specifications	44	57	The solution should support OS like VIOS, Red Hat, Ubuntu etc.	Request NABARD to modify the clause as below: "The solution should support OS like Red Hat, Ubuntu etc" Justification: With VIOS, multiple solutions can be routed via proxy settings. However, since VIOS is not a commonly used OS, not all vendors provide agent-based solutions — and this might breach the tamper-proof clause. Also, please advise on the below : i) How many systems are VIOS, Ubuntu and RedHat... ii) Is this end user device or Servers? iii) Are these systems in the office network ?	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					iv) Does NABARD has SAML authentication like ADFS etc ?	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
81	Scope of Work and Technical Specifications	44	59	The solution should be supporting customized reporting, scheduled reporting, etc where daily weekly monthly should be scheduled.	Request NABARD to change the clause as below: "The solution should be supporting reporting with scheduled reporting, etc where daily weekly monthly should be scheduled. Custom reporting is not required, as the extensive set of built-in reports fully meets the needs for both granular and enterprise-level analysis, ensuring simplicity and efficiency without the need for complex customization."	No change
82	Scope of Work and Technical Specifications	77	54	The platform should be able to provide the details of internet-facing assets with Visualization graphs to cover below scope: 1. Discovered root domains 2. Hosts 3. Ips 4. Assets by location 5. Domain's discovery trends over the period of last 12 months	Request NABARD to consider moving this clause under the EASM section, as it aligns more appropriately with the features and capabilities of an EASM solution.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
83	General			Additional Point	Request NABARD to confirm if the capabilities of EDR, NBAD, SOAR and SIEM can be offered with a unified platform, that allows significant benefits over and above individual point products offering similar capabilities.	No Change
84	General			Additional Point on SIEM	Request NABARD to confirm the retention requirements for log storage and whether long term storage needs to be provisioned as part of the SIEM product or externally for archival	Please refer to the RFP
85	Scope of Work and Technical Specifications	26	64	The system must manage user activity by host over time even when username doesn't present in the immediate event data.	Request to modify as "The system should monitor and alert on anomalous user activity over time even if the username is not present in immediate event data by performing cross platform analytics", since managing user activity is not under the scope of an SIEM.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
86	Scope of Work and Technical Specifications	28	11	UBA should activate a rule for a set of users until a specified condition or specified time window.	It is not recommended to create static conditions for overriding analytics detections since this can bring down efficacy of analytics detections. Request to modify this as "UBA should perform continous baselining of all User, Identity, Network and Endpoint behaviour across peers for quickly identifying and alerting anomalous behaviour"	No change
87	Scope of Work and Technical Specifications	44	1	The solution should have inbuilt user behaviour machine learning based scoring mechanism.	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
88	Scope of Work and Technical Specifications	44	2	DAM Solution should provide easy & fast deployment It should be available as a predeployed virtual appliance which could be deployed on hypervisor like Nutanix, VMware etc.	Kindly requesting to amend the statement as; "DAM Solution should provide easy & fast deployment. It should be available as a pre-deployed virtual applianceor software based installation which could be deployed on hypervisor like Nutanix, VMware etc."	Kindly refer to corrigendum
89	Scope of Work and Technical Specifications	44	5	DAM Solution should have bidirectional integration available with Standard SIEM solution	Requesting to share the business use case for the given ask for better understanding.	Kindly refer to the RFP
90	Scope of Work and Technical Specifications	44	6	DAM Solution should integrate with all type of known databases in the organization	Requesting to share list of Database type and the major + minor versions to check the compatibility.	Same shall be shared with the successful bidder.
91	Scope of Work and Technical Specifications	44	7	Automatically deploy sensor agents across DB environment using centralized implementation manager dashboard. Turn sensors on/off from single console.	Kinldy requesting to amend the clause as; "Automatically/manually deploy sensor agents across DB environment using centralized implementation manager	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					dashboard or with manual installation. Turn sensors on/off from single console."	
92	Scope of Work and Technical Specifications	45	17	Allow drill down into the actual SQL being executed by users on any of the databases being monitored.	Requesting to share the use case for the given ask for better understanding.	Please refer to the RFP
93	Scope of Work and Technical Specifications	45	19	Configure local agent settings from management interface on appliance	Requesting to share the use case for the given ask for better understanding.	Kindly refer to the RFP
94	Scope of Work and Technical Specifications	45	20	Create an audit compliance workflow for a few users allowing for comments, escalation and signoff.	Request to remove the Clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
95	Scope of Work and Technical Specifications	45	21	If applicable, monitor local database activity that uses Named Pipes	Request to remove the Clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No Change
96	Scope of Work and Technical Specifications	45	25	Classify data in databases according to pre-defined rules on GDPR, PCI, and SOX criteria	Classify data in databases according to pre-defined rules on GDPR, PCI, and SOX criteria	Kindly refer to the RFP
97	Scope of Work and Technical Specifications	45	26	Capture and Report on Database Entitlements	Requesting to share the business use case for the given ask for better understanding.	Kindly refer to the RFP
98	Scope of Work and Technical Specifications	45	30	Group objects (sensitive and financial) and activities for use in reporting. Test autopopulation of groups through a query or LDAP connection	Group objects (sensitive and financial) and activities for use in reporting. Test autopopulation of groups through a query or LDAP connection	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
99	Scope of Work and Technical Specifications	45	32	Define an audit review process, selecting a group of three reports and send via email for review and signoff.	Request to remove the Clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	Kindly refer to corrigendum
100	Scope of Work and Technical Specifications	45	34	Review all SQL exceptions, including all failed SQL commands. Send these as reports. (Either automatically as a report card report or audit workflow).	Requesting to share the business use case for the given ask for better understanding. Specify the classification functionality	Please refer to the RFP
101	Scope of Work and Technical Specifications	46	44	Selectively alias technical information for less technical audiences.	Requesting to share the business use case for the given ask for better understanding.	Please refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
102	Scope of Work and Technical Specifications	46	45	If applicable, monitor local database activity that uses Oracle Bequeath.	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change
103	Scope of Work and Technical Specifications	46	46	The solution should Mask and redact critical information stored on DB when accessed directly by DBA	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change
104	Scope of Work and Technical	46	48	The solution should Automatically analyze installed policies for evaluating the effectiveness and performance.	Requesting to share the business use case for the given ask for better understanding.	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
	Specifications					
105	Scope of Work and Technical Specifications	46	49	The solution should perform User behavioral analytics highlighting working hours and off hour activity, with observations and severity.	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change
106	Scope of Work and Technical Specifications	46	50	Highlight any anomalous activities based on observed patterns	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
107	Scope of Work and Technical Specifications	46	51	Export risky user behavior to PDF or CSV files and create a review process to automatically distribute reports on a schedule.	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
108	Scope of Work and Technical Specifications	46	54	Proposed DB Vulnerability Assessment (VA) solution should enable the facility of scanning data infrastructures (databases, data warehouses and big data environments) to detect vulnerabilities, and suggest remedial actions. The solution should identify exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Full reports should be provided along with suggestions to address all vulnerabilities. It should detect behavioural vulnerabilities such as account sharing, excessive administrative logins and unusual after- hours' activity. It should identify threats and security gaps in databases that could be exploited by hackers. Proposed DB VA solution shall facilitate: - Automated discovery of unknown data assets - Sensitive data classification in data sources - Entitlements and data source credentials	Kinldybrequesting to amend the statement as; "Proposed DB Vulnerability Assessment (VA) solution should enable the facility of scanning data infrastructures (databases, data warehouses and big data environments) to detect vulnerabilities, and suggest remedial actions. The solution should identify exposures such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Full reports should be provided along with suggestions to address all vulnerabilities. It should identify threats and security gaps in databases that could be exploited by hackers."	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				monitoring - Automated vulnerability scanning and configuration - Mapping of predefined tests for best practice standards - Behavioural vulnerabilities exposure - Behavioural vulnerabilities exposure		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
109	Scope of Work and Technical Specifications	47	56	The solution must have protection capabilities like Masking and Redaction in addition to traditional access control / firewall policies that DBA systems provide	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change
110	Scope of Work and Technical Specifications	47	57 and 58	Proposed DAM solution must have proactive approach or provide visibility to advanced threats and with the ability to proactively correlate activities and give insights into the following kinds of attacks: a) SQL injection b) Malicious stored procedure c) Data leak d) Denial of service e) Account take-over f) Schema tampering g) Data tampering h) Anomaly	Kindly requesting to amdn the statement as: "Proposed DAM solution must have proactive approach or provide visibility to advanced threats and with the ability give insights into the following kinds of attacks: a) SQL injection b) Malicious stored procedure c) Schema tampering d) Data tampering"	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
111	Scope of Work and Technical Specifications	47	59	The DAM solution must have AI / ML capability to dynamically assess risk factors and use a smart algorithm to identify potential risks across entire system. None of these AI / ML features should be dependent on using any 3rd party and must be entirely driven by standalone DAM product. However, when integrated with a SOAR, SOC, Identity Management and other systems the value of such analysis should gain further reach	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change
112	Scope of Work and Technical Specifications	47	62	The solution must be able to monitor traffic from cloud hosted databases or Database as a service real time with minimal footprint and can be leverage on modern containerised architecture like Kubernetes services.	Requesting to share list of Database type and the major + minor versions to check the compatibility.	Same shall be shared with the successful bidder.
113	Scope of Work and Technical Specifications	47	66	The solution should be able find, classify, secure, monitor, visualize, and manage a customer's data security needs. Additionally, it has open interfaces and integrations with the rest of the security and IT solutions.	Requesting to mention what level of integrations are required.	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
114	Scope of Work and Technical Specifications	47	68	The solution must support consolidation of the audit logs and send to data insight solution that can be used for fast reporting and analytics over long retention periods	Need more clarity.	Kindly refer to the RFP
115	Scope of Work and Technical Specifications	48	70	The solution must be able to highlight the top risky users, database based on the usage pattern and identifies anomalies by using outlier mining (including the volume of outliers, the severity of individual events, the predicted volume of outliers for a specific time of day)	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
116	Scope of Work and Technical Specifications	48	71	The solution must be able to detect threat pattern based on series of event not just based on single query and support detection of below threat category: a) Account Takeover b) Anomaly behaviours c) Brute Force Attack d) Cross-site scripting (XSS) e) Data tampering f) Denial of Service g) Insider threat: possible data leak h) Malicious stored procedure i) massive grants j) OS command injection k) Schema tampering l) SQL injection (general \Tautology\Side channel\Denial of Service)	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change
117	Scope of Work and Technical Specifications	48	73	The solution should provide an internal workflow capability that allows users to raise issues and assign them to other users.	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					The same functionality can be achieved with the SIEM/SOAR platform.	

118	Scope of Work and Technical Specifications	48	76	The solution must support zero trust principle (i.e. Never trust always verify) and perform continuous verification of all incoming connection while leverage on AI/ML to cover various scenario and also categorized connection as trusted/untrusted. The AI/ML must leverage on below criteria during evaluation of connection metadata: a) A new OS client connected to a database server. b) A new OS user connected to a database server. c) A new Client connected to a database server. d) A new database user connected to a database server. e) An unexpected combination of OS user and database user was detected. f) An unknown DAM agent is found for this Server IP address. g) Client connected using unexpected authentication type. h) The DAM agent detected an unknown or unexpected database type. i) unexpected authentication used for this database. j) Unexcepted client time zone	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change

				detected k) Unexcepted command was used at the connection start l) Unexcepted error at connection start		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
119	Scope of Work and Technical Specifications	49	78	The solution must support end to end data security lifecycle like Discovery, Classification, Vulnerability Assessment, Real-time and Passive monitoring, agent based and agent less option, Entitlement reporting of database access.	Kindly requesting to amend the clause as; " The solution must support end to end data security lifecycle like Discovery, Classification, Vulnerability Assessment, Real-time and Passive monitoring, agent based or agent less option, Entitlement reporting of database access"	No change
120	Scope of Work and Technical Specifications	49	79	The solution must provide Vulnerability Assessment for wide range of database (onprem/Cloud hosted – Oracle, SQL Server, MySQL, SAP HANA, SAP Sybase, Teradata, Maria DB, Mongo DB, DB2 or Database as a Service like AWS RDS support for Oracle, SQL Server, MySQL, PostgreSQL)	Kinldy requesting to amend the clause as; "The solution must provide Vulnerability Assessment for wide range of database (on-prem/Cloud hosted - Oracle, SQL Server, MySQL, SAP HANA, SAP Sybase, Maria DB, Mongo DB, DB2 or Database as a Service like AWS RDS support for Oracle, SQL Server, MySQL, PostgreSQL)."	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
121	Scope of Work and Technical Specifications	49	81	The solution should be able to support advance data security by integrating with Data Governance Catalog tools and provide Query Rewrite support to help with dynamic masking of return data.	Request to remove the clause Justification: Not all leading Database Security solution OEM offers behaviour and machine learning technology with the prposed solution, hence requesting to remove this point for the maximum participation. The same functionality can be achieved with the SIEM/SOAR platform.	No change
122	Scope of Work and Technical Specifications	63	24	The solution should provide management as a service	Request for Clarifications: Request to share more details on the use case for this clause	Same shall be shared with the successful bidder.
123	Scope of Work and Technical Specifications	63	35	Solution should be aligned and supported to the latest OS releases	Requesting to share list of current OS types	Same shall be shared with the successful bidder.
126	Scope of Work and Technical Specifications	65	66	The solution will enforce prohibited Applications and Files based on the compliance settings by monitoring for the presence of specified files, registry values, and processes that are prohibited to be	Request to modify clause as Solution will allow only whitelisted applications on the endpoint. Allother applications will be blocked by default	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				running or present on endpoint computers.	without any modofication to the policy	
127	Scope of Work and Technical Specifications	65	67	The solution will enforce an Anti-Malware check to verify that computers have an antimalware program installed and updated	Request to modify that Solution will check if Antimalware is deployed or not	The Bidder to provide antimalware solution as a part of EPP
59	Scope of Work and Technical Specifications	65	69	The solution will be used to determine if users can connect to wireless networks while on your organization's LAN to protect the network from threats associated with wireless networks.	Request NABARD to remove this clause Justification: Endpoint protection platforms (EDR) offer behavioral detection and response capabilities, but wireless enforcement typically falls under NAC or Zero Trust agents. It is not designed to control or enforce wireless adapter behavior or detect dual connections (Wi-Fi + LAN) natively.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
128	Scope of Work and Technical Specifications	65	69	The solution will be used to determine if users can connect to wireless networks while on your organization's LAN to protect the network from threats associated with wireless networks.	Request to remove the Clause Justification: The mentioned technical clause is of NAC and not part of EPP/EDR	Kindly refer to corrigendum
317	Scope of Work and Technical Specifications	65	69	The solution will be used to determine if users can connect to wireless networks while on your organization's LAN to protect the network from threats associated with wireless networks.	Request NABARD to remove this clause Justification: Endpoint protection platforms (EDR) offer behavioral detection and response capabilities, but wireless enforcement typically falls under NAC or Zero Trust agents. It is not designed to control or enforce wireless adapter behavior or detect dual connections (Wi-Fi + LAN) natively.	Kindly refer to corrigendum
60	Scope of Work and Technical Specifications	65	70	The solution will define if users can connect to the organization network from hotspots in public places, such as hotels or airports.	Request NABARD to Remove this clause Justification: Defining access based on network type is not typically part of an XDR’s scope but is effectively addressed by integrating VPN, firewall, and	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					posture-check mechanisms along with the XDR platform.	
129	Scope of Work and Technical Specifications	65	70	The solution will define if users can connect to the organization network from hotspots in public places, such as hotels or airports	Request to remove the Clause Justification: The mentioned technical clause is of NAC and not part of EPP/EDR	Kindly refer to corrigendum
131	Scope of Work and Technical Specifications	66	90	The solution must lock the user from using files until they are checked and found to be benign	Request to remove the Clause Justification: The mentioned technical clause is of NAC/VPN and not part of EPP/EDR	No change
132	Scope of Work and Technical Specifications	66	98	When scrubbing, the original file must be accessible by end user if is found to be benign by the sandbox	Requesting to share the business use case for the given ask for better understanding.	use case shall be shared with the successful bidder.
133	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	Can you please mention total number of applications that will be protected using WAF solution?	Same shall be shared with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
134	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The proposed Cloud WAF solution should have 99.999% SLA for service availability.	No change
135	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The solution should have capability to protect multiple website, Protect Application with Custom Ports	No Change
136	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The proposed solution should protect all the parts of API (header, body, query parameters, methods) against a broad scope of API threats, including data leakage, denial of service, automated threats (bots), embedded attacks, etc. The protection should be adaptive for both documented and undocumented APIs based on automated API discovery that requires no application or security expertise.	No Change
137	Scope of Work and Technical	10	3.5	Web Application Firewall as a Service Additional Point	Solution should support out-of-path deployment mode without need to share SSL certificates	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
	Specifications				and the integration should be API-based to reduce latency.	
138	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	Solution should support out-of-path deployment mode without need to share SSL certificates and the integration should be API-based to reduce latency.	No change
139	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The solution should have full-fledged BOT protection from Day-1 with following capabilities: (i) Defend against BOTs that target digital assets, including sophisticated BOTs designed to hit multiple assets. (ii) Detect and identify BOTs using multi-layered approach, including signatures of known BOTs, HTTP profiling, device fingerprinting, CAPTCHA or better mechanism, behavioral challenges and semi-supervised machine learning. (iii) Detect and block sophisticated human like BOTs in real time with no impact on	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					the technology stack. (iv) Identify the intent of the BOTs with the highest precision through proprietary, semi supervised machine learning models.	
140	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	Solution should provide SDK to integrate with iOS & Android apps to ensure safety against identity spoofing, identity tampering & replay attacks. Also the provided SDKs should be able to embed into native applications & developed ones using React Native Framework.	No change
141	Scope of Work and Technical	10	3.5	Web Application Firewall as a Service Additional Point	Solution should support mobile attestation for both iOS & Android devices to prevent BOT attacks on mobile devices	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
	Specifications					
142	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The solution should be able to detect bad BOTs like Misbehaving legitimate BOTs, BOT attacking from public cloud, known bad BOTs, Scripted BOTs, Programmatic session behavior, Advanced java script validation failure, malicious browser behavior, low & slow attacks, malicious intent detection.	No change
143	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The solution should possess attack mitigation methods like blocking of user or session, feed fake data to BOTs, filter the traffic, throttle or rate based blocking, sesison termination, redirect loop to the bad BOTs, challenge captcha mitigation, any other customisation as per the application requirement.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
144	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The BOT management solution must have the attack detection and mitigation mechanism as core feature like collective BOT intelligence, IP reputation to track proxy & TOR request, semi-supervised machine learning to identify emergent BOT patterns, user behavior analysis for anomaly detection, dynamic reverse tuning test to uncover bot identity, unique device fingerprinting creation, global deception network.	No Change
145	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	Solution should provide mitigation based on Cryptographic challenge by detecting anomalous behavior of bad BOT solving captchas.	No change
146	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	Should support the capability to collects more than 250 client-side and server-side parameters for accurate detection.	No change
147	Scope of Work and Technical	10	3.5	Web Application Firewall as a Service Additional Point	Solution should be able to work as standalone or into application stack via different options:	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
	Specifications				SDKs, JS tag, API cloud connectors, web server plug-ins.	
148	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	Solution should support private access tokens	No change
149	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The proposed WAF Solution must have Positive Security Model supporting advanced behavior-analysis technologies to separate malicious threats from legitimate traffic.	No change
150	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	Security Related standards for OEM owned DDoS Scrubbing Center Service Datacenter ISO/IEC 27001:2013, ISO/IEC 27032:2012 ISO 28000:2007 PCI-DSS v4.0 US SSAE16 SOC-1 Type II, SOC-2 Type II ISO 9001:2008, ISO 22301:2012, ISO 14001:2004,	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					ISO 50001:2011 , OHSAS 18001:2007	
151	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	Please advise based on the specifications/features mentioned for WAF solution, a SaaS based Cloud WAF solution can also be proposed.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, Cloud based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
						active-active mode at all the sites.
152	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service Additional Point	The solution should provide full BOT protection to the applications.	No Change
153	Scope of Work and Technical Specifications	62	1	The solution should be present in the market for more than 5 years.	What specific documentation or evidence will be required from bidders to demonstrate that their proposed solution has been present in the market for more than 5 years?	Declaration from OEM is required.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
154	Scope of Work and Technical Specifications	62	6	Solution must have a deeply functional and documented API to support integration and automation across the platform and with other platforms	Please provide information regarding the required integration of security tools.	Kindly refer to the RFP
155	Scope of Work and Technical Specifications	62	11	Granular control of policy based on group/device/user	kindly consider Granular control of policy based on group/device	No change
156	Scope of Work and Technical Specifications	63	15	The solution should allow running a remote PowerShell script on the client.	kindly consider to add playbook function for remote query execution.	No change
157	Scope of Work and Technical Specifications	62	10	Ability to completely stop the antivirus/EPP during application installs.	Please consider to remove this clause as endpoint should active all time.	No change
158	Scope of Work and Technical Specifications	63	26	Solution must have backups provided as part of the service Solution must be GDPR compliant	kindly consider to remove this clause as the solution is not deploy in euro region.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
159	Scope of Work and Technical Specifications	64	54	Solution must have a strong partner sharing community	Please provide information regarding the required parameter.	Kindly refer to the RFP
160	Scope of Work and Technical Specifications	64	60	Users will log on one time (SSO) for authentication to the operating system, Full Disk Encryption, and other Endpoint Security blades.	Please consider solution should have authentication to the operating system, Full Disk Encryption, and other Endpoint Security blades.	Kindly refer to corrigendum
161	Scope of Work and Technical Specifications	68	136	The solution must be integrated with Bank's TIP solution	Please provide information regarding the existing TIP platform.	Bidder to provide fresh new TIP solution as specified in the requirements.
162	General			Additional Point	What is the current SIEM solution in use (product, version, license, expiry)	Bidder has to provide a new solution altogether.
163	General			Additional Point	Is any SOAR tool already deployed If yes, share product details.	Bidder has to provide a new solution altogether.
164	General			Additional Point	If SIEM/SOAR exists, what is the migration plan for old log data	Bidder has to provide a new solution altogether.
165	General			Additional Point	Can we get the split of 10K EPS total for DC, DR, Near DR, or separate for each	A Cumulative of 10K EPS is expected across the three sites

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
166	General			Additional Point	Will DR and Near DR run active-active or only during failover	All the sites will function in HA in Active-Active mode.
167	General			Additional Point	Architecture diagram showing sites, log sources, and security devices	Same shall be shared with the successful bidder.
168	General			Additional Point	List of log sources to integrate (fi rewalls, servers, DBs, AD, cloud, banking, email, third-party)and estimated log volume per source type	Please refer to the RFP
169	General			Additional Point	Are custom parsers needed for any logs	Please refer to the RFP
170	General			Additional Point	Will NABARD provide test/dev infra for integration	Please refer to the RFP
171	General			Additional Point	Does NABARD use any Threat Intelligence feeds now Should they be integrated	Bidder has to provide a new solution altogether.
172	General			Additional Point	Are there existing SOAR playbooks to migrate	Bidder has to provide a new solution altogether.
173	General			Additional Point	Where should the SOC team operate from — NABARD site, bidder's SOC, or hybrid	No onsite manpower is envisaged. However, NABARD may request the team to be physically present during meetings.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
174	General			Additional Point	Are there minimum onsite manpower requirements	No onsite manpower is envisaged. However, NABARD may request the team to be physically present during meetings.
175	General			Additional Point	What report formats and dashboards are expected for daily/weekly/monthly SOC tracking	Reports format and dashboard shall be prepared by Bidder in consultation with NABARD.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
176	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/OSCP/ CEH certified. Note: (i) Resources for CEHMax 10 resources shall be considered. The certification date must be prior to the date of	We already havea team of 50+ Security Practice, 20+ Certifi ed SIEM SME's (Microsoft Sentinel Certifi ed) & 1CEH. We being MSME registered vendor we hope we shall be considered under eligibilitycriteria	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				publication of this RFP. (ii) If a resource is carrying more than one certification, it shall be considered as one.		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
177	Scope of Work and Technical Specifications	68	6	Network Detection and Response (NDR)/NBAD solutions take advantage of the flow technologies built into network devices. NDR /NBAD tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs data into meaningful analytics data like numbers charts and tables that quantify exactly how the network is being used, by whom and for what purpose.	Requesting Clause Change to Network Detection and Response (NDR)/NBAD solutions take advantage of the flow technologies built into network devices and must also support full packet capture (PCAP) and smart capture for enhanced visibility. NDR /NBAD tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs and packet data into meaningful analytics data like numbers, charts, and tables that quantify exactly how the network is being used, by whom and for what purpose. Justification: Request inclusion of full packet capture (PCAP) and smart capture support in addition to flow-based data. Flow data lacks application & payload visibility and limits deep forensic investigations,	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					encrypted threat detection, and protocol-level reconstruction. Packet data enables complete network visibility, historical traffic analysis, and compliance-driven retention, making it essential for accurate threat detection and incident response.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
178	Scope of Work and Technical Specifications	69	17	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.	Requesting Clause Change to The solution should support all forms of standard flow formats including but not limited to NetFlow, IPFIX, sFlow, Jflow, and must also support Full Packet Capture (PCAP) for comprehensive,visibility, forensic investigation, and compliance-driven retention. Justification: NSEL (NetFlow Secure Event Logging) is a Cisco-proprietary protocol specifically designed for exporting security event logs from Cisco ASA firewalls. It is not a vendor-neutral standard and may exclude OEMs that do not support Cisco-specific telemetry. In contrast, Full Packet Capture (PCAP) is a vendor-agnostic approach that enables the collection of complete network traffic, including headers and payloads. PCAP can be used to derive	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					metadata similar to flow records while also supporting deep forensic analysis, encrypted threat detection, protocol reconstruction, and long-term retention. To maintain vendor neutrality and enhance visibility, we request to remove NSEL and include PCAP support.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
179	Scope of Work and Technical Specifications	72	68	The solution must be able to provide visibility of user endpoint workstations and support & service options to collect telemetry from these endpoints including username, process names and process hashes involved in the network traffic. If there is any License to be provided, the same should be considered for 50 endpoint workstations from day one.	Request to delete the clause from NDR/NBAD specifications Justification: The described functionality collecting telemetry such as process names, hashes, and usernames from endpoints is a core feature of Endpoint Detection and Response (EDR) solutions. NBAD/NDR tools are agentless designed to monitor network traffic passively and do not natively collect endpoint-level telemetry without an endpoint agent. This clause may unintentionally restrict participation of standalone NBAD/NDR vendors, especially when EDR/XDR is already a separate part of the RFP scope. Also, as per Pt. No. 8 of NBAD Compliance, the solution is expected to provide contextual, network-wide visibility via an agentless approach, which directly contradicts this	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					endpoint telemetry requirement. We request to either remove this clause from the NDR section or move it under the EDR scope where endpoint telemetry requirements are appropriately handled.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
180	Scope of Work and Technical Specifications	70	40	The solution must detect unusual, unauthorized behaviour within the network. This includes but is not restricted to unusual RDP, port scanning, unauthorized new devices plugged in, unauthorized use of access credentials to internal resources.	Requesting Clause Change to The solution must detect unusual network behaviors such as RDP anomalies, port scanning, and lateral movement. Unauthorized device detection and credential misuse should not be included under the NDR scope. Justification: NBAD/NDR solutions are capable of detecting network anomalies like unusual RDP activity or port scanning. Please note that detections such as "unauthorized new devices plugged in" or "unauthorized use of access credentials" typically require telemetry from NAC and IAM systems correlated at SIEM level. These are not native to NDR platforms. We request removal of these points to ensure technical alignment with the scope of network-based detection.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
181	Scope of Work and Technical Specifications	73	99	The solution should have an automated scanner to identify assets and should also be able to schedule the scans	Request to remove the clause from NDR/NBAD scope. Justification: The described functionality of automated and scheduled scanning for asset identification is a core feature of Vulnerability Assessment (VA) scanners, not NDR/NBAD solutions.	Kindly refer to corrigendum
182	Scope of Work and Technical Specifications	73	100	The solution should allow taking logs from proxy and enrich that to flows for showing users behind the proxies.	Request to remove the clause to maintain vendor neutrality. Justification: This is a vendor-specific clause favoring flow-based solutions. PCAP-based NDR platforms natively offer user/session visibility. Additionally, enabling X-Forwarded-For (XFF) headers on proxy devices can also achieve the same objective without requiring log ingestion.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
183	Scope of Work and Technical Specifications	71	59	Ability to detect ransomwares and profiling malwares such as Troldesh, Dridex, Quakbot, TrickBot, Gootkit, Adware, TorrentLocker, Adwind, Tofsee, Gozi, Jbifrost, Dyre, ZeuS Gameover, chinad, bamital, Post Tovar GOZ, corebot, cryptominers, etc	Requestion Clause Change to The solution should be able to detect and monitor ransomwares and malwares.	No Change
184	Scope of Work and Technical Specifications	74	105	The solution should have native integration with CERT CMTX & NCIIPC Threat Feeds	Requesting Clause Change to The solution should support ingestion of threat feeds from CERT CMTX & NCIIPC via global standards such as STIX/TAXII.	Kindly refer to corrigendum
185	Scope of Work and Technical Specifications	74	103	The solution should have native integration with any PDNS service to obtain unlimited DNS resolution and domains hosted information along with WHOIS directly from the portal	Request to remove the clause. Justification: This is a vendor-specific capability not supported by all NDR/NBAD solutions. It is also not a core requirement for network detection and response. We request removal of this clause to maintain vendor neutrality and avoid restricting participation.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
186	QCBS Evaluation Criteria	4	B.2.(J)	The proposed NBAD solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	The proposed NBAD solution should have been supplied and implemented by OEM in at least 5 banking organizations in India in the last five years (FY 2020–2021 to FY 2024–2025), Service Experience: (a) 5 references and above- 4 marks (b) 3 to 4 references -3 marks (c) 2 to 3 references- 2 marks	Kindly refer to corrigendum
187	Scope of Work and Technical Specifications	68	9	Network Behavior Anomaly Detection (NBAD) Additional Point	Add a clause specifying required metadata retention period and peak network throughput (in Gbps) for DC, DR, and Near DR locations for proper solution sizing.	No change
188	Scope of Work and Technical Specifications	68	9	Network Behavior Anomaly Detection (NBAD) Additional Point	Request for Addition The solution should be a dedicated behaviour analytics solution delivering advanced Network detection and Response (NBAD/NDR) use cases and not a subset capability of SIEM and SOAR.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
189	Scope of Work and Technical Specifications	68	9	Network Behavior Anomaly Detection (NBAD) Additional Point	Request for Addition: The solution should provide an integrated Malware analysis engine to emulate malware or any unknown malicious object, file etc. seen in the network communication to provide defense against advanced and sophisticated network-borne threats.	No change
190	Scope of Work and Technical Specifications	68	9	Network Behavior Anomaly Detection (NBAD) Additional Point	Request for Addition: The solution must provide a comprehensive capability for retrospective network analysis using full packet to understand the sequence of events enabling identification , investigations and remediation of network anomalies and security incidents based on historical data.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
191	Scope of Work and Technical Specifications	68	9	Network Behavior Anomaly Detection (NBAD) Additional Point	Request for Addition: The NDR platform shall include a fully integrated, native IDS engine that provides thousands of CVE-mapped signatures at no additional hardware or software cost, with unrestricted inspection of both North-South and East-West traffic.	No change
192	Scope of Work and Technical Specifications	68	9	Network Behavior Anomaly Detection (NBAD) Additional Point	Request for Addition: The solution should be able to generate reconstructed PCAP files for designated time periods using session or metadata information, supporting incident investigation and analysis.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
193	Project Timelines and Deliverables	2	D6	Operations & Maintenance M1 + 45 days onwards	This shows O&M should start from M1+45 Days where M is month from the date of PO which is contradictory to Project Timelines table which states that O&M to start from Go Live which is understood from earlier table as T+45 days. Also these both clauses are contradictory to GeM notification "Contract Period" which is mentioned as 5 years, because with clauses in Project Timelines and Deliverables document the contract duration is either 5 years 45 days or 5 years 75 days (i.e. M1+45 days). Kindly amend accordingly.	No change
194	General				Please allow extension of atleast 4-6 weeks from date of publishing of query responses.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
195	Scope of Work and Technical Specifications	1	2.(a)	The bidder must deliver managed security services for NABARD, ensuring that the entire solution is deployed at NABARD designated locations on pay-as-you-go model. This approach aims to ensure that NABARD's infrastructure is both secure and scalable, meeting the organization's evolving needs over the contract period.	Please suggest if bidder is required to provide hardware and related tools as "1. Introduction/a" or only software tools with services as mentioned in "2. Brief Scope of Work/a,b" at NABARD specified locations i.e. DC, DR and Near Site as both clauses are contradictory to each other. Kindly clarify and amend accordingly.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
196	Scope of Work and Technical Specifications	17	9	Responsibility Matrix	As per the RACI matrix, infrastructure is to be provided by the MSP. Could you please clarify if there are any mandated public or private cloud providers, or if the MSSP is permitted to host services on any compliant cloud provider within India.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
197	Minimum Eligibility Criteria	2	7	Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024- 25, FY 2023-24, 2022- 23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches (This shall override experience criteria given in the bid in other documents)	As per the eligibility criteria, we understand that the proposed solution must include SIEM (supporting 10,000 EPS), SOAR, and at least four components mentioned in the RFP. We request clarification on whether this condition can be relaxed to allow experience in SIEM support more broadly, considering that most MSSPs and Global SIs work across multiple technologies. Restricting eligibility to only specific toolsets may limit participation and exclude otherwise qualified providers with relevant large-scale experience.	Global POs may be considered. However, the bidder has to abide by the Clause 7.(b) of the Minimum Eligibility Criteria as prescribed in the corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
198	Project Timelines and Deliverables	1	2	Installation, configuration and commissioning of the tools T+45 Days	The current clause specifying a T + 45 days timeline for implementation appears to be quite aggressive, considering the time required to complete internal formalities such as booking the order in the system and initiating the onboarding and integration of various log sources. We would request to consider relaxing this clause, allowing for a more realistic and achievable implementation schedule, in alignment with practical deployment timelines and system readiness.	No change

199	QCBS Evaluation Criteria	2	B.(1)	Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22, 2020-21 (Bidder shall submit PO/credential letters) a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks Further, the bidder shall submit the customer's feedback form having positive feedback, as attached in Annexure I, against the submitted PO/credential letters and the marks allocated against the same are as below: a) 02 projects - 3 Marks b) 03 projects - 4 Marks c) 04 projects - 5 Marks Additionally, if the submitted POs as per the above criteria pertain to the BFSI clients, additional marks as below shall be allocated a) 03 to 05 projects - 3 Marks	Requesting NABARD to remove the minimum 4 solutions/ tools proposed with SIEM +SOAR. Also to revise the SIEM and SOAR solutions separately. Request to revise the customer feedback form counts from 4 projects to 2 for 5 marks and submitted POs from 8 projects and above to 3 to 4 projects.	No Change

				b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks		

200	QCBS Evaluation Criteria	###	B.(2)	(A) The proposed SIEM solution with a minimum of 10000 EPS should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 7 marks (b) 13 to 14 references -5 marks (c) 10 to 12 references- 3 marks (B) The proposed SOAR + TIP solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (C) The proposed WAF solution with should have been supplied and implemented by OEM in India in last five years(FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023- 2024, FY 2024-2025): Service Experience:	Requesting NABARD to relax the reference counts for point # A-J from 15 references to 3-4 references.	Kindly refer to corrigendum

				(a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (D) The proposed DAM solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (E) The proposed SWG solution with should have been supplied and implemented by OEM in India in last five years(FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (F) The proposed PAM solution with should have been supplied and implemented by OEM in India in last five years(FY 2020-2021,		

				FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (G) The proposed EDR solution with should have been supplied and implemented by OEM in India in last five years(FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks (H) The proposed EASM solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 3 marks (b) 13 to 14 references -2 marks (c) 10 to 12 references- 1 marks (I) The proposed SCM solution		

				with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 3 marks (b) 13 to 14 references -2 marks (c) 10 to 12 references- 1 marks (J) The proposed NBAD solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/contract agreement/ work order/ engagement letter/invoices/signoff Letter.		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
201	Scope of Work and Technical Specifications	10	3.5	Web Application Firewall as a Service	Can you please mention total number of applications that will be protected using WAF solution?	Bidder shall provide the WAF solution on the basis of troughput only.
202	Scope of Work and Technical Specifications	2	(h)	The bidder will be responsible for providing deployment and 24*7*365 operational support for all the security tools proposed in this RFP	We understand that the RFP mentions a 24x7 service window. We would appreciate your clarification on the following: For the components listed under the scope of work, can the bidder propose a 24x7 support model exclusively for the SoC functions—namely SIEM, SOAR, and related monitoring services—while offering business hours support for other components, with on-call support for Severity 1 issues outside of business hours example PAM, DAM,WAF etc ? Kindly confirm	Bidder shall propose 24x7 support mode for all the in scope solutions in the RFP.
203	Scope of Work and Technical Specifications	61	29	Risk score should be based on accepted industry metrics, and allow for customization	Its based on CVSS and differential log Deduction, Customization please elaborate as platform is Built on AI/ML and assign score based on ,	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					assets and Vulnerability and take care of all incident Severity	
204	Scope of Work and Technical Specifications	60	17	Solution should discover assets across all cloud providers	We provide services across all three major cloud platforms — AWS, GCP, and Azure — and ensure full compliance with their respective standards. Kindly confirm where the bank's infrastructure is currently hosted.	The Bank's infrastructure is currently hosted on a Private Cloud setup
205	Scope of Work and Technical Specifications	61	56	The solution should provide compliance dashboards that map identified Issues to compliance frameworks to help our teams understand their overall compliance with regulatory and organizational policies. These dashboards need to provide executive visibility, prioritize high-risk cybersecurity areas, and measure the progress of our organization's maturity.	At present, customization of the risk score by the customer is not supported. However, the CloudSEK platform is built on an AI/ML-driven engine that automatically prioritizes risks based on severity levels — High, Medium, and Low. Additionally, incidents can be classified as False Positive, Informational, or Irrelevant, and based on these classifications, they can be	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					assigned to the respective team members for appropriate action.	
206	Scope of Work and Technical Specifications	62	68	The Solution should perform data gathering activity of IT assets frequently (on daily/weekly basis) and should be updated in the console in an automated manner. Perform attack surface assessment of third-party vendors / service providers	We Discussed during Pre-Bid its only for NABARD Atatck Surface Visbily on not any third pearty vendors	The solution should also gather data from Third party vendors also.
207	Scope of Work and Technical Specifications	61	34	Solution should have the ability to automatically remediate exposures. This should include full resolution of the incident by reaching back via API and blocking the service at the port level.	Our ESSM platform can be seamlessly integrated with the bank's SIEM and SOAR systems. Once integrated and aligned with the appropriate playbooks, the desired use cases can be effectively achieved.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
208	Minimum Eligibility Criteria	2	7	Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024- 25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches (This shall override experience criteria given in the bid in other documents)	The Experience of registered partner may also be considered. As All such solutions are not available with single TSP.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
209	Minimum Eligibility Criteria	3	8	The bidder should have its own/ Captive New Generation SOC Setup in India (technology and customer logs should be stored in Indian jurisdiction only) providing SOC as a service/ managed SOC services including remote log monitoring, correlation and analysis and security incident management services, etc	The SOC services are provided with partnership of OEMs and vendors, so the certification of partner along with bidder may also be considered	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
210	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/CREST/ CISM/ CISA/ OSCP/ CEH certified. Note: (i) Resources for CEHMax 10 resources shall be considered. The certification date must	The SOC services are provided with partnership of OEMs and vendors, so the certification of partner along with bidder may also be considered	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				be prior to the date of publication of this RFP. (ii) If a resource is carrying more than one certification, it shall be considered as one.		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
211	Minimum Eligibility Criteria	4	10	The bidder should have support office in India for 24x7x365	The NOC is run by OEM or the partners of TSP, so same should be accepted for eligibility	No Change
212	Project Timelines and Deliverables	1	1	Procure and supply solution components at DC, DR & Near site T+1 Months	Request to change Procure and supply solution components at DC, DR & Near site T+ 2 Months	No change
213	Project Timelines and Deliverables	1	2	Installation, configuration and commissioning of the tools T+45 Days	Request to change Installation, configuration and commissioning of the tools T + 75 Days	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
214	Service Level Agreement	37	3.1	SLAs for Security Solutions viz. SIEM, SOAR, WAF, DAM, SWG, PAM, EDR, EASM, TIP, SCM, NBAD on individual basis Uptime Availability of each of the Security Tools Minimum 99.982% up time measured on a monthly basis for individual security tool penalty impack level Nil >= 99.8% to <99.982% up time measured on a monthly basis for individual security tool Penalty impact level 5 Penalty 6% >= 99.7% to <99.8% up time measured on a monthly basis for individual security tool Penalty Impact Level-6 Penalty 7% >= 99.6% to <99.7% up time measured on a monthly basis for individual security tool Penalty impact level-7 Penalty 8% >= 99.5% to <99.6% up time measured on a monthly basis for individual security tool Penalty impact level -8 Penalty 9% <99.50% up time measured on a	Request to change Uptime Availability of each of the Security Tools Minimum 99.982% up time measured on a monthly basis for individual security tool penalty impack level -Nil >= 99.8% to <99.982% up time measured on a monthly basis for individual security tool Penalty impact level 1 Penalty 2% >= 99.7% to <99.8% up time measured on a monthly basis for individual security tool Penalty Impact Level-2 Penalty 3% >= 99.6% to <99.7% up time measured on a monthly basis for individual security tool Penalty impact level-3 Penalty 4% >= 99.5% to <99.6% up time measured on a monthly basis for individual security tool Penalty impact level -4 Penalty 5% <99.50% up time measured on a monthly basis for individual security toolPenalty impact level -5 Penalty 6%	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				monthly basis for individual security toolPenalty impact level -9 Penalty 10%		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
215	Service Level Agreement	42	3.6	Incidence ResponseThe Solution should be able to tackle the incidence and provide the response as soon as the incidence is detected <=30 mins Impact level Nil >30 mins and <=60 mins impact level 7 Penalty 8% >60 mins and <=90 mins impact level 8 penalty 9% >90 mins and <=180mins impact level 9 Penalty 10%	Request to change Incidence ResponseThe Solution should be able to tackle the incidence and provide the response as soon as the incidence is detected <=30 mins Impact level Nil >30 mins and <=60 mins impact level 1 Penalty 2% >60 mins and <=90 mins impact level 2 penalty 3% >90 mins and <=180mins impact level 3 Penalty 4%	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
216	Minimum Eligibility Criteria	2	7	Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024-25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches (This shall override experience criteria given in the bid in other documents)	We request NABARD to consider below point, considering it as managed service. 7 Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of SIEM with minimum of 10k EPS and SOAR, and any 2 among PAM, EDR, NBAD, DAM, WAF, SWG, TIP, DNS Security, SCM,EASM,Endpoint Security) for atleast 3 distinct clients in the last 5 years (FY 2024- 25, FY 2023-24, 2022- 23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 900+ branches (This shall override experience	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					criteria given in the bid in other documents)	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
217	Minimum Eligibility Criteria	2	7	1. PO indicating the value from customers for managed SOC (Along with the declaration of the proposed tool to that client) And 2. Completion certificate / Sign off certificate from the client (for the submitted POs) if project is completed. 3. In case of NDA signed between the bidder and the client, bidder may submit masked PO with the declaration of tools, services and value of the PO.	PO indicating the value from customers for managed SOC (Along with the declaration of the proposed tool to that client)	Kindly refer to corrigendum
218	Minimum Eligibility Criteria	3	8	The bidder should have its own/ Captive New Generation SOC Setup in India (technology and customer logs should be stored in Indian jurisdiction only) providing SOC as a service/ managed SOC services including remote log monitoring, correlation and analysis and security incident management services, etc.	The bidder should have its own/sister/Subsidiary company/ Captive New Generation SOC Setup in India (technology and customer logs should be stored in Indian jurisdiction only) providing SOC as a service/ managed SOC services including remote log monitoring, correlation and analysis and security incident management	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					services, etc.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
219	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH certified. Note: (i) Resources for CEHMax 10 resources shall be considered. The certification date must	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH certified/CompTIA Security+/ISO 27001 Certified/ ISO/IEC 27001:2022 Note: (i) Resources for CEH- Max 15 resources shall be considered. The certification	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				be prior to the date of publication of this RFP. (ii) If a resource is carrying more than one certification, it shall be considered as one.	date must be prior to the date of publication of this RFP. (ii) If a resource is carrying more than one certification, it shall be considered as one.	

220	QCBS Evaluation Criteria	2	B.(1)	Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22, 2020-21 (Bidder shall submit PO/credential letters) a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks Further, the bidder shall submit the customer's feedback form having positive feedback, as attached in Annexure I, against the submitted PO/credential letters and the marks allocated against the same are as below: a) 02 projects - 3 Marks b) 03 projects - 4 Marks c) 04 projects - 5 Marks Additionally, if the submitted POs as per the above criteria pertain to the BFSI clients, additional marks as below shall be allocated a) 03 to 05 projects - 3 Marks	Request NABARD to consider below clause: Bidder can submit only successfull completion or satistfactory certificate for feedback. Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22,2020-21 (Bidder shall submit PO/credential letters.) a) 03 to 05 projects - 5 Marks b) 06 to 07 projects - 10 Marks c) 08 projects and above - 15 Marks	No Change

				b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
221	QCBS Evaluation Criteria	4	C	Scoring Criteria for bidder Certifications: a. ISO27001 Certification - 2 Marks b. Cert-in Empanelment - 2 Marks c. SOC II Type II Certification - 1 Marks All these certifications should be valid as on 1st April 2025	Scoring Criteria for bidder Certifications: a. ISO27001 Certification - 2 Marks b. Cert-in Empanelment - 2 Marks c. SOC II Type II Certification of Bidder or its Sister Company - 1 Marks All these certifications should be valid as on 1st April 2025. SOC II Type II Certificate is given to the Data Center/Cloud where SOC is hosted. Request you to kindly consider the SOC II Type II Certificate of the Data Center/Cloud where Bidder's SOC is hosted.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
222	QCBS Evaluation Criteria	4	D	The bidder must have IT Security resources on permanent payroll having experience in-scope solutions with Certifications such as CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) 50 to 75 resources- 04 marks (b) 76 and above resources- 09 marks Note: (i) Resources for CEH- Max 10 resources will be considered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource has more than one certification, it will be considered as one. (iii) Of the above, the bidder must have a total of 5 certified resources of the proposed SIEM solution on permanent payroll. If not, then the count of resources will not be considered, and no marks shall be awarded under Clause 'D'.	The bidder must have IT Security resources on permanent payroll having experience in-scope solutions with Certifications such as CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH //CompTIA Security+/ISO 27001 Certified/ ISO/IEC 27001:2022 (a) 50 to 75 resources- 04 marks (b) 76 and above resources- 09 marks Note: (i) Resources for CEH- Max 15 resources will be considered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource has more than one certification, it will be considered as one. (iii) Of the above, the bidder must have a total of 5 certified resources of the SIEM solution on permanent payroll.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					If not, then the count of resources will not be considered, and no marks shall be awarded under Clause 'D'.	

223	Scope of Work and Technical Specifications	2	2.(d)	Integration of components (hardware/software) with each other and the Bank's Infrastructure and with third party devices is the sole responsibility of the selected bidder. Besides, the bidder has to ensure that their tools are integrated in the Bank's /its Cloud provider portals viz., SLA portal, Invoice portal, Service Desk portal, Bird's eye view Dashboard etc	We request NABARD to consider below requirement for Bird's eye view Dashboard. The bidder shall provide an integrated, web-based dashboard with role-based customized views, offering a secure online portal for real-time visibility into incidents/events, alerts, action statuses, and related updates a. High-level overview of the most critical security metrics and KPIs, enabling the NABARD and other stakeholders to make informed decisions. b. Top Alerts/Threats - Dedicated section on the Security dashboard to display the top alerts, top attacks in an environment, users/hosts under attack and threats with visual indicators such as charts or graphs to represent the volume and severity of alerts. c. Incident Response Metrics – Total number of security incidents detected within a specific period. d. True Positive vs False Positive	Kindly refer to the RFP

					– Comparative analysis on generating TP vs FP over specific period. e. Active Devices Count – Dashboard should provide real time information on active devices sending logs vs failure devices. f. Compliance Metrics/Reports – The solution must provide overall compliance status with relevant regulations and standards (e.g. CERT-IN, RBI, PCI-DSS Guidelines etc.) with in the security dashboard portal. T	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
224	Service Level Agreement	37	3.1	SLAs for Security Solutions viz. SIEM, SOAR, WAF, DAM, SWG, PAM, EDR, EASM, TIP, SCM, NBAD on individual basis	Request NABARD to confirm if NMS solution will be provided for up time management of solution hosted at NABARD premise	NMS solution is already provisioned by MSP. However MSSP shall integrate all security solutions infra on NMS.
225	Scope of Work and Technical Specifications	1	2	Brief Scope of Work	Bidder understand hardware/virtual machine for hosting these RFP solution will be provided by NABARD. Please confirm our understanding	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
226	Scope of Work and Technical Specifications	1	1.(a)	The RFP seeks to engage a Managed Security Service Provider (MSSP) for providing managed SOC services across the proposed Bank's Infrastructure which consists of Private Cloud spanning across DC, DR and near Site. This includes the procurement of necessary hardware and related tools, as well as the ongoing operations and management of the entire Security solution. The entire solution has to be maintained over a five-year period from the go live date. NABARD may further extend the contract beyond a term of 5 years on a mutual agreement basis.	1. We understand SIEM/ SOAR and other solutions will be MSSP/ cloud deployment, please confirm. 2. We understand NABARD will provide the necessary VMs/ HW/ Connectivity at their DC, DR, NDR for deployment of Log Collectors / Flow collectors/ Agents for SIEM deployed in MSSP/ Cloud model.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
227	Scope of Work and Technical Specifications	1	2.(b)	The solution shall include Supply, Installation, Implementation, Integration, Roll Out, Operations and Maintenance of all the security tools listed in this RFP in DC, DR and Near site for the entire contract duration:	Since the entire scope is offered as a service, request you to remove the supply of hardware and licenses condition from RFP clause. The entire offering will be delivered to you as a service with all local hardware/ infra requirement to be provided by NABARD.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
228	Scope of Work and Technical Specifications	3	t	Service Window - Bidder will assign a service management team for the duration of the Contract and a "Single point of contact (SPOC)" should be assigned for all servicerelated matters to NABARD/its authorized persons and should be able to respond within the designated service window. The proposed "Service managers" should be a multi-skilled professional and supported by back-end support as required with 24 X 7X 365 expected Service Window. Bidder should ensure that they should be accessible by means of 24x7 Phone Support, 24x7 Messaging and Via Email	Please confirm if the resources can be provided in a cost effective Hybrid model with PMO on-site and rest remotely from bidder facility.	Resources managing the entire setup can provide the services remotely.
229	Scope of Work and Technical Specifications	4	jj	Bidders must provide access to all the tools proposed in the RFP to NABARD.	Since this is a service based offering with SLAs, request you to remove the clause of providing read/write access to NABARD	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
230	Scope of Work and Technical Specifications	5	3.1.5	The bidder must provide the bank with read/write access to the SIEM platform	Since this is a service based offering with SLAs, request you to remove the clause of providing read/write access to NABARD, instead we will provide read only access and write access will be provided on-demand basis temporarily.	No change
231	Scope of Work and Technical Specifications	8	3.3.10	The bidder shall be responsible for Reporting and logging of information security incidents through the use of Bank's ticketing tool	What is your ITSM tool with version ? Does it support API integration with SIEM/ SOAR and other technologies.	Same shall be shared with the successful bidder. However, the tools does support API Integration
232	Scope of Work and Technical Specifications	13	3.11.2	The NBAD solution shall be seamlessly integrated with the Bank's existing infrastructure and network devices and the proposed solutions such as AD, SIEM, Firewalls etc. The integration shall be carried out by the bidder.	Can we consider 5000 FPS at each location (DC & DR)	Please refer to BOM and Commercials
233	Scope of Work and Technical Specifications	23	3		Please remove this clause for Video learning content on SIEM solution, no SIEM vendors provides a learning module.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
234	Scope of Work and Technical Specifications	23	5	The solution must support auto discovery of assets that are being protected or monitored and make them available in an asset database within the system	Auto-discovery modules of SIEMs are not effective, we request to meet this requirements through integrating VM services which will perform discovery scans in a much accurate and effective way.	No change
235	Scope of Work and Technical Specifications	23	12	Solution must be able to store logs in a separate system which would not be required to perform any real time correlation thereby minimizing the load on the Real time analysis	Please explain your requirement for separate log storage, is this non-cyber compliance logs. What is the volume of logs to be stored per day in GBs ? Who will provide the storage solution to store these logs ?	Please refer to the RFP. All the storage requirements shall be fulfilled by NABARD.
236	QCBS Evaluation Criteria	2	B.2.(A)	The proposed SIEM solution with a minimum of 10000 EPS should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 7 marks (b) 13 to 14 references -5 marks (c) 10 to 12 references- 3 marks	Since it's a managed service, request you to remove the clause of "supplied' for all solutions under scope.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
237	QCBS Evaluation Criteria	2	B	Experience Clause	For experience of proposed solutions only OEM experience is required, please confirm.	Kindly refer to corrigendum
238	Payment Terms and Conditions	1	2	Payment shall be made on a quarterly basis, in arrears.	We request to change the payment clause to 50% yearly in advance to incorported the platform and licenses charges which are paid upfront to OEM.	No change
239	Scope of Work and Technical Specifications	10	3.5.5	The minimum application throughput WAF must be 300 Mbps	What are the expected performance metrics for the WAF solution beyond the minimum application throughput of 300 Mbps? Are there specific latency or response time requirements?	Kindly refer to the RFP
240	Scope of Work and Technical Specifications	10	3.5.4	Bidder to supply and implement Web Application Firewall (WAF) with a centralized dashboard that should provide real time incident response, reporting and monitoring. The solution should have the migration capability from on premises to Cloud	Can you provide more details on the migration process from on-premises to cloud? Are there specific cloud platforms that the WAF solution should be compatible with?	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
241	Scope of Work and Technical Specifications	10	3.5.10	In case there is a requirement of integration of WAF solution with any existing or new security device/solution, within the contract period the same is to be done by the bidder without any cost to the Bank	In the event of new security devices or solutions being introduced, what is the expected timeline for integration? Are there any specific processes that need to be followed?	Same shall be shared with the successfule bidder.
242	Scope of Work and Technical Specifications	13	3.10.4	The solution should be deployed at 500 endpoints (OS included)	Is the requirement for deploying the solution at 500 endpoints a fixed number, or is there potential for scaling in the future? If scaling is needed, what would be the expected number of endpoints?	Kindly refer to the RFP
243	Scope of Work and Technical Specifications	16	6.(A)	Bidder shall arrange the training for all proposed services/ tools by the OEMs proposed as part of the RFP. The topics should cover detailed functionality, configurations, troubleshooting etc of its product	Please confirm if the training is expected to be done onsite or remote	Training can be provided either in physical mode at NABARD's site or in virtual mode
244	Scope of Work and Technical Specifications	15	5.(a)	The bidder along with the solution provided shall comply with the following standards:	Request you to confirm the deliverable for this exercise and frequency of the same	NABARD may ask MSSP bidder to submit any compliance documents or supporting materials specified by the authorities (specified in

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
						clause 5.a) at any time during the project period.
245	Scope of Work and Technical Specifications	17	9	Responsibility Matrix VAPT (before go live)	Request you to confirm the scope and activities to be done under this point	MSSP to fix /mitigate VAPT recommendations provided by VAPT team during entire project tenure.
246	GeM Bid Document			EMD Amount - Rs.60,00,000/- (Rupees Sixty Lakhs)	We wish to highlight that we have annual turnover of more than ₹ 500 Crore, in all of the past three completed. financial years. We are exempt from submitting the bid security as per the General Terms & Condition on GeM 4.0 (Version 1.23) dated 5th March 2025 (Clause 4.xiii.(m).v).shows we are exempt from submitting the EMD for this RFP. Request you to please confirm the same that we can submit our bid without submitting the EMD	Please refer to the GEM guidelines

247	Scope of Work and Technical Specifications	15	4	4. Audit/Health Check a) The bidder shall arrange an annual health check of all the proposed security solutions by OEM. The coordination with OEM for completion of Health checks is Bidders responsibility. All costs associated with the audit/Health check shall be borne by the bidder. Bidder has to submit an independent Health check report for all security solutions with NABARD. The health check shall cover the following things but not limited to: · Configurations of security solutions · User access review of all tools · Acceptance testing/ audit of bidder deliverables · Review of Exit Management, Strategic Controls · Usability Compliance b) Bidder shall also allow NABARD to Audit/review the setup remotely and/or On Site by its own team and/or by any 3rd party Auditor appointed by NABARD on regular basis c) Bidder shall fix the gaps, if any, observed before the go-live and	We propose changes in the existing clause as below:- Audit/Health Check:- a) The bidder shall arrange an annual health check of all the proposed security solutions by OEM. The coordination with OEM for completion of Health checks is Bidders responsibility. All costs associated with the audit/Health check shall be borne by the bidder. Bidder has to submit an independent Health check report for all security solutions with NABARD. The health check shall cover the following things but not limited to: ·Configurations of security solutions · User access review of all tools · Acceptance testing/ audit of bidder deliverables · Review of Exit Management, Strategic Controls · Usability Compliance Provided that NABARD shall give 10 working days' prior written notice for any such health check or audit activity requiring bidder's coordination or response. b) Bidder shall also allow	No Change

				during the project cycle on the basis of the observations found by VAPT /SOC/IS/any other audit team. d) Bidder shall assist third party auditor/ NABARD Auditor for security related queries as and when required during the project tenure. e) The bidder shall conduct a one-time independent audit of the entire solution by a third-party auditor prior to sign-off. The auditor must be appointed with prior approval from NABARD. If NABARD is not satisfied with the auditor proposed by the bidder, NABARD reserves the right to appoint an alternative auditor. All costs associated with the audit, regardless of whether the auditor is appointed by the bidder or NABARD, shall be borne by the bidder. The audit report submitted by the independent auditor will serve as the basis of Sign off document for the go-live.	NABARD to Audit/review the setup remotely and/or On Site by its own team and/or by any 3rd party Auditor appointed by NABARD on regular basis.Such audit shall be conducted during normal business hours and with the reasonable prior notice of 10 working days. c) Bidder shall fix the gaps, if any, observed before the go-live and during the project cycle on the basis of the observations found by VAPT /SOC/IS/any other audit team. d) Bidder shall assist third party auditor/ NABARD Auditor for security related queries as and when required during the project tenure. e) The bidder shall conduct a one-time independent audit of the entire solution by a third-party auditor prior to sign-off. The auditor must be appointed with prior approval from NABARD. If NABARD is not satisfied with the auditor proposed by the bidder, NABARD reserves the right to appoint an alternative auditor. All costs associated with the audit,	

					regardless of whether the auditor is appointed by the bidder or NABARD, shall be borne by the bidder. The audit report submitted by the independent auditor will serve as the basis of Sign off document for the go-live.	

248	Non-Disclosure Agreement	6 and 7	7	7. Remedies 7.1. The System Integrator acknowledges the confidential nature of Confidential Information and breach of any provision of this Agreement by the System Integrator will result in irreparable damage to NABARD for which monetary compensation may not be adequate and agrees that, if it or any of its directors, officers or employees should engage or cause or permit any other person to engage in any act in violation of any provision hereof. NABARD shall be entitled, in addition to other remedies for damages & relief as may be available to it, to an injunction or similar relief prohibiting the Implementation partner, its directors, officers etc. from engaging in any such act which constitutes or results in breach of any of the covenants of this Agreement. Any claim for relief to NABARD shall include NABARD's costs and expenses of enforcement (including the attorney's fees). 7.2. Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized used or disclosure of Confidential	We propose changes in the existing clause as below:- Remedies:- 7.1. The System Integrator acknowledges the confidential nature of Confidential Information and breach of any provision of this Agreement by the System Integrator will result in irreparable damage to NABARD for which monetary compensation may not be adequate and agrees that, if it or any of its directors, officers or employees should engage or cause or permit any other person to engage in any act in violation of any provision hereof. NABARD shall be entitled, in addition to other remedies for damages & relief as may be available to it, to an injunction subject to applicable law and due process or similar relief prohibiting the Implementation partner, its directors, officers etc. from engaging in any such act which constitutes or results in breach of any of the covenants of this Agreement,However, any such relief shall be proportionate and based on sufficient evidence of	No Change

				Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party, and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use. 7.3. Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at Disclosing Party's request, or at Disclosing Party's option,certify destruction of the same. 7.4. Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies (as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction. a. Suspension of access privileges b. Change of personnel assigned to the job	actual breach Any claim for relief to NABARD shall include NABARD's costs and expenses of enforcement (including the attorney's fees). Provided that the System Integrator shall be given reasonable notice and an opportunity to cure such breach, wherever curable, before any injunctive or punitive action is initiated. 7.2. Receiving Party shall notify Disclosing Party immediately upon discovery of any unauthorized used or disclosure of Confidential Information and/ or Confidential Materials, or any other breach of this Agreement by Receiving Party, and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and/ or Confidential Materials and prevent its further unauthorized use. 7.3. Receiving Party shall return all originals, copies, reproductions and summaries of Confidential Information or Confidential Materials at	

				c. Financial liability for all direct damages which disclosing party has incurred as a result of a finally determined breach of the terms of this agreement by the Recipientor its employees or advisors or representatives. d. Termination of contract 7.5. Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.	Disclosing Party's request, or at Disclosing Party's option,certify destruction of the same.Such return or destruction shall be completed within a reasonable time frame (e.g., 30 working days), subject to any applicable legal, regulatory, or archival obligations. 7.4. Receiving Party acknowledges that monetary damages may not be the only and / or a sufficient remedy for unauthorized disclosure of Confidential Information and that disclosing party shall be entitled, without waiving any other rights or remedies (as listed below), to injunctive or equitable relief as may be deemed proper by a Court of competent jurisdiction. a. Suspension of access privileges b. Change of personnel assigned to the job c. Financial liability for all direct damages which disclosing party has incurred as a result of a finally determined breach of the terms of this agreement by the Recipientor its employees or advisors or	

					representatives.(provided that indirect, incidental, or consequential damages are excluded unless arising from willful misconduct or gross negligence) d. Termination of contract 7.5. Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
249	Service Level Agreement			Additional Point	We reccomend to add new clause under the RFP:- Termination by Bidder:- In the event NABARD 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 NABARD, the bidder may terminate this defenitive Agreement or any portion thereof or the applicable statement of work by giving written notice to the NABARD.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
250	Service Level Agreement			Additional Point	We reccomend to add new clause under the RFP:- Non-Solicitation:-During the Term of this Definitive Agreement and for a period of one year thereafter, neither Party shall (either directly or indirectly through a third party) solicit to employ, cause to be solicited for the purpose of employment to any employee/s (including the employees who have been exposed or introduced to other Party during initial discussion between Parties or engaged to provide/perform the services under any definitive agreement entered between Parties) of the other Party or aid any third person to do so, without the specific written consent of the other Party. The said restriction shall also apply to each Party's affiliates, agents, vendors, contractors, and any third parties with whom such Party has a relationship (collectively,	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					"Representatives"). Parties agree that Representatives are equally restricted from poaching or soliciting or inducing any employees of other Party to leave their employment or engagement with such other Party.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
251	Service Level Agreement			Additional Point	We recommend to add new clause under the RFP as below:- Force Majure:- Neither Party shall be liable for any delay or failure in performance of its obligations under this Agreement if such delay or failure results from events beyond its reasonable control, including, without limitation, acts of God, earthquakes, riots, terrorism, war, fire, epidemics, or other similar circumstances ("Force Majeure Event"). The obligations and rights of the affected Party shall be extended on a day-to-day basis for the duration of the Force Majeure Event. If the performance of either Party is delayed by a Force Majeure Event for more than thirty (30) days, the other Party may terminate this Agreement or the affected Purchase Order or Statement of Work for convenience by providing	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					written notice to the affected Party	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
252	Service Level Agreement			Additional Point	We recommend to add new clause under the RFP as below:- Limitation of Liability :- Notwithstanding any other provision hereof, neither party shall be liable for any indirect, incidental, special, consequential, exemplary or punitive damages or any damages for lost profits, lost revenues, loss of goodwill, loss of anticipated savings, loss of customers, or loss of data, or interference with business, arising out of the performance or failure to perform under this Contract, whether or not caused by the acts or omissions or negligence (including gross negligence or willful misconduct) of its employees or agents, and regardless of whether such party has been informed of the possibility or likelihood of such damages. In no event, regardless of the form of the claim or cause of action (whether based in contract,	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					negligence, strict liability, tort or otherwise) shall either party's aggregate liability to the other party exceeds the fees/amount actually paid by NABARD to the Service Provider in the twelve (12) months preceding the event giving rise to the claim.	
253	Scope of Work and Technical Specifications	11	3.6.5	The Solution should be able to maintain logs for a duration of 6 months on the server and in archival for the entire contract duration.	As per industry best practice , we recommended to have online storage for 3 Month and archival of Log for contract Duration.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
254	Scope of Work and Technical Specifications	10	3.6	Database Activity Monitoring (DAM) as a service	Request you to please provide thenumber of DB instancea and type for sizing the DAM Solution	The same shall be shared with the successful bidder.
255	Minimum Eligibility Criteria	2	7	Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024- 25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches (This shall override experience criteria given in the bid in other documents)	We request to modify the clause as below:- Experience a) The bidder should have experience of providing Managed SOC Services either onpremises or remote 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM/PIM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024-25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					having more than 1000 branches. (This shall override experience criteria given in the bid in other documents)	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
256	Minimum Eligibility Criteria	2	7	Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024- 25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches (This shall override experience criteria given in the bid in other documents)	Please confirm whether separate POs can be used for different solutions.	Kindly refer to corrigendum Multiple POs for a minimum of 4 solutions, issued by the same client in last 5 years can be considered.

257	QCBS Evaluation Criteria	2	B.(1)	Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22,2020-21 (Bidder shall submit PO/credential letters) a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks Further, the bidder shall submit the customer's feedback form having positive feedback, as attached in Annexure I, against the submitted PO/credential letters and the marks allocated against the same are as below: a) 02 projects - 3 Marks b) 03 projects - 4 Marks c) 04 projects - 5 Marks Additionally, if the submitted POs as per the above criteria pertain to the BFSI clients, additional marks as below shall be allocated a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks	Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 3 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and any 2 among (SOAR, PAM/PIM, EDR, NBAD/NDR/PCAP, UEBA/UBA, DAM, WAF, SWG, TIP/TIF, SCM, EASM) in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22,2020-21 (Bidder shall submit PO/credential letters) a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks Further, the bidder shall submit the customer's feedback form having positive feedback, as attached in Annexure I, against the submitted PO/credential letters and the marks allocated against the same are as below: a) 02 projects - 3 Marks b) 03 projects - 4 Marks	No Change

				c) 08 projects and above - 5 Marks	c) 04 projects - 5 Marks Additionally, if the submitted POs as per the above criteria pertain to the BFSI / Govt. clients, additional marks as below shall be allocated a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks	

258	QCBS Evaluation Criteria	2	B.(1)	Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22,2020-21 (Bidder shall submit PO/credential letters) a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks Further, the bidder shall submit the customer's feedback form having positive feedback, as attached in Annexure I, against the submitted PO/credential letters and the marks allocated against the same are as below: a) 02 projects - 3 Marks b) 03 projects - 4 Marks c) 04 projects - 5 Marks Additionally, if the submitted POs as per the above criteria pertain to the BFSI clients, additional marks as below shall be allocated a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks	Please confirm whether separate POs can be used for different solutions.	Multiple POs for a minimum of 4 solutions, issued by the same client in last 5 years can be considered. However such multiple POs shall be considered as a single project for the purpose of evaluation.

				c) 08 projects and above - 5 Marks		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
259	QCBS Evaluation Criteria	4	C	Scoring Criteria for bidder Certifications: a. ISO27001 Certification - 2 Marks b. Cert-in Empanelment - 2 Marks c. SOC II Type II Certification - 1 Marks All these certifications should be valid as on 1st April 2025.	Request to consider previous year certificate if FY24-25 SOC II Type II Certificate is under audit.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
260	QCBS Evaluation Criteria	4	D	The bidder must have IT Security resources on permanent payroll having experience in-scope solutions with Certifications such as CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) 50 to 75 resources- 04 marks (b) 76 and above resources- 09 marks Note: (i) Resources for CEH- Max 10 resources will be considered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource has more than one certification, it will be considered as one. (iii) Of the above, the bidder must have a total of 5 certified resources of the proposed SIEM solution on permanent payroll. If not, then the count of resources will not be considered, and no marks shall be awarded under Clause 'D'.	We request that certification from the Security Solutions OEMs be considered, as it is essential for ensuring expertise in daily operations. Request to remove cap on CEH rescources.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
261	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH certified. Note: (i) Resources for CEH- Max 10 resources shall be considered. The certification date must be prior to the date of publication of this RFP.	We also request that certification from the Security Solutions OEMs be considered, as it is essential for ensuring expertise in daily operations. Request to remove cap on CEH rescources.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				(ii) If a resource is carrying more than one certification, it shall be considered as one.		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
262	Scope of Work and Technical Specifications	13	3.10.2	The Web Proxy solution shall be seamlessly integrated with the Bank's existing infrastructure devices and the proposed solution such as AD, SIEM and Firewalls, etc. The integration shall be done by the bidder.	Web Proxy solution is obsolete product and Secure Service Edge is the new technology inline with Web Proxy. Hence request to change clasue as "The Web Proxy solution/SSE shall be seamlessly integrated with the Bank's existing infrastructure devices and the proposed solution such as AD/ADFS, SIEM and Firewalls, etc. The integration shall be done by the bidder."	No Change
263	Scope of Work and Technical Specifications	13	3.10.5	The solution shall include Web Proxy with Caching, Web Content Filtering, URL filtering, Application layer filtering, Application control features, etc	In today's dynamic web page/content it will not provide any benefit to have a cache the content. SSE or next-gen web proxy solution provides faster respose to applications by edge computing and prallel processing. Hence request to change clasue for maximum OEM participation and adoption of new technology to NABARD. The solution shall include Web Proxy with Web Content Filtering, URL filtering, Advance Threat Protection, BoT	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					protection, CnC, Application layer filtering, Application control features, etc.	
264	Scope of Work and Technical Specifications	40	3	Solution should have SSO/MFA for admin users for console login page.	SSE or Web Proxy solution create policy based on the users not based on IP address, Hence request you to add SSO/MFA for the not obly admins but for all 500 users. Hence request to change clasue as "Solution should have SSO/MFA for SSE/Web proxy users and admin users for console login page. MFA/SSO OTP must be delivered through SMS or Email. "	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
265	Scope of Work and Technical Specifications	41	13	Hardware & software (if needed) be installed at Bank premises for the provision of the services along with syncing the Meta data for AD attributes	AD doesnot support the federation service for third party tool over SAML, SAML 2.0 is universal authentiocation protocol supported by ADFS and Next-Gen Web Proxy/SSE solution. Hence request to change clasue as "Hardware & software /ADFS(if needed) be installed at Bank premises for the provision of the services along with syncing the Meta data for AD attributes. Proposed solution must support SAML-2.0 for authentication"	No change
266	Scope of Work and Technical Specifications	41	15	The solution should have authentication options for users/groups. It should supports authentication of users via Integrated Windows Authentication, NTLM (NTLM v1 and v2 in Session Security), and LDAP.	As SSE and Next-gen web proxy suppoort integration through SAML for authentication of the web proxy agent. NTLM authentcioation is not required for SSE solution. Hence request to change clasue as "The solution should have authentication options for users/groups. It should supports authentication of users via SAML and LDAP."	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
267	Scope of Work and Technical Specifications	42	25	Solution should have built in various reports and should be able to create custom reports like Executive report, Investigative report, Top 10 reports for various category and Health reports etc	For bank it is essential to have the report which can be presented to CISO and CIO from from security incidents and visbility of overall security posture of the Bank. Hence request to modify clasue as "Solution should have built in various reports and should be able to create custom reports like Executive report, Investigative report, Top 10 reports for various category and Health reports . The solution should have built in various reports and should be able to create custom reports like Executive CISO report, Investigative report, Top 10 reports for various category and Health reports etc and should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time).etc."	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
268	Scope of Work and Technical Specifications	42	30	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links, etc.	SSE or Web Proxy solution will inspect the traffic from all assests hence request to change clasue as "The proposed solution should support to monitor/inspect traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links, etc."	Kindly refer to corrigendum
269	Scope of Work and Technical Specifications	43	41	The agent on server machines should be tamperproof, for example, the agent cannot be uninstalled by the user even with admin rights to the system or the user cannot stop the services.	In tempre proof apart from unistall Bank must include logout and disable, so that security is always on on end user machine. Hence request to change clause as "The agent on server machines should be tamperproof, for example, the agent cannot be uninstalled, logout and disable by the user even with admin rights to the system or the user cannot stop the services. If user need to logout, disable or uninstall admin will provide OTP specific to user not global password"	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
270	Scope of Work and Technical Specifications	44	57	The solution should support OS like VIOS, Red Hat, Ubuntu etc	This clasue is restricting us from particiaption. Hence request to change clasue as "The solution should support OS like Windows, macOS, openSUSE, Red Hat, Ubuntu, iOS, Android and ChromeOS etc."	Kindly refer to corrigendum
271	Scope of Work and Technical Specifications	40	4	Secure Web Gateway (SWG) /Web Proxy Additional Point	Request to add This feature will help bank to valdiate the posture of the devcie before providing acces to the internet which will add addtional layer of security to check the psoture of device. Hecne request to add this clause " The device posture check must validate Certificate Trust, File Path, Registry Key, Client Certificate, Domain Joined, Process Check, firewall, Encryption, Detect Antivirus along with AV signature update, OS Version before providing access to application."	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
272	Scope of Work and Technical Specifications	40	4	Secure Web Gateway (SWG) /Web Proxy Additional Point	Request to add DNS is the one of the vulnerable protocol which is used by cyber criminals for CnC and data exfilteration. Hence request to add clause as "The proposed Solution must have DNS Security feature from day 1 to secure internet traffic. The DNS Security Solution should have all DNS controls including request and response categorizations, tunnel detection, resolved IP based countries and inspect DNS over HTTPS (DoH) etc. extended for all DNS requests."	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
273	Scope of Work and Technical Specifications	40	4	Secure Web Gateway (SWG) /Web Proxy Additional Point	Request to add Browser isolation will provide the capability to isolate user traffic if user access any malicious website. IF user download any malicious file it will not be dwonload on user machine it will be download on isolated enviournment. Hence request to change cl;asue as "The proposed solution should support daily categorization for customer's top 100 unknown domains. The solution must have a Smart Browser Isolation policy that automatically isolates potentially malicious web content using the AI/ML models which continually identify suspicious domains to stop phishing attacks"	No change
274	Scope of Work and Technical Specifications	40	2	The solution should have ability to protect the sensitive data exfiltration based on geolocation.	This use case can be addressed with DLP. Is the DLP solution required by the OEM, or if integration with an existing DLP is needed.	Please refer to the RFP. Bidder has to provide a new DLP solution for the proposed setup.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					Which DLP solution NABARD is currently using?	
275	Scope of Work and Technical Specifications	40	4	The solution should provide, Expanded Internet access for off-site users in real-time for the Hybrid Offsite Roaming users from day 1, without the need to connect the user to office.	a. Does NABARD require hybrid solution? b. If going with Hybrid mode, what on premises platform would NABARD prefer for Proxy deployment? 1. VM (if VM do NABARD provide required compute resources). 2. Dedicated Hardware appliance by OEM	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
276	Scope of Work and Technical Specifications	41	10	The solution must not be a "single point of failure" in network traffic flow; the failure of one or more components of the solution should not affect the organizational network's functionality.	Please Clarify? 1. is the on-prem deployment mode HA between DC and DR or. 2. HA at DC only? 3. This clause applicable only for on-prem appliances / solution.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.
277	Scope of Work and Technical Specifications	41	11	The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability malicious content of password and unknown encryption files.	Request to change : The solution should provide geo-location awareness for security incidents. The solution should provide inbuilt capability to detect malicious content. Justification: any sandbox cannot break password protection or decrypt unknown encrypted files. we can detonate	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					the password protected sample with known password if any	
278	Scope of Work and Technical Specifications	41	17	The solution should have support of multiple domains, the administrators can specify the sequence (Domain controllers checked first, second, next, etc.) used to authenticate users who login from different locations.	1. This is typically a function of Active Directory (AD) configuration. Request to provide more clarity on this requirement. 2. Request you to relax this clause / requirement as it is limited to a specific OEM.	No change
279	Scope of Work and Technical Specifications	42	18	The solution should have Multi-Domain authentication to allow the admin to create rules that authenticate against multiple domain controllers in a sequence	The sequence and priority of domain controllers are generally managed automatically by Active Directory.	No change
280	Scope of Work and Technical	42	24	Solution should provide reports with (but not limited to) HTML/CSV/PDF formats.	Request to change: Solution should provide reports with CSV/PDF formats.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
	Specifications				As Major OEM's suuport this formats.	
281	Scope of Work and Technical Specifications	42	30	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links, etc.	as part of SWG/SSE solution the traffic of the users can be monitored. Please elaborate the use case for monitor traffic for better understanding.	Kindly refer to corrigendum
282	Scope of Work and Technical Specifications	44	57	The solution should support OS like VIOS, Red Hat, Ubuntu etc.	Is this a requirement for corporate users , Servers or roaming users?	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
283	Scope of Work and Technical Specifications	10	3.5.5	The minimum application throughput WAF must be 300 Mbps.	1. We kindly request NABARD team to modfy this clause as "The commercial proposal should be based on FQDNs inclusive of unlimited WAF and L3-L7 DDoS (bandwidth) per FQDNS with addon options for API Security requests/month and Bot protection for transaction/month" 2. Please clarify on the requirement: Do we need to propose virtual WAF appliance of 300Mps, so that NABARD will host on VM/Cloud instance. If Yes, specify the number of virtual appliance requirement. If you are loking for SaaS based Cloud WAF. The licensing will be based on FQDN (Fully qualified Domain Name).	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
284	Scope of Work and Technical Specifications	38	8	The commercial proposal should be based on FQDNs inclusive of unlimited WAF and L3-L7 DDoS (bandwidth) per FQDNS with addon options for API Security equests/month and Bot protection for transaction/month	1. We kindly request NABARD team to clarify, "Total number of FQDNs to be onboarded for WAF on Day One." 2. We kindly request NABARD team to clarify, "For API Security, we would need the total number of FQDNs requiring API Discovery and the estimated number of API requests per month for API Protection. Please confirm if the commercial details for the add-on license are required to be shared on Day One."	Kindly refer to corrigendum
285	Scope of Work and Technical Specifications	10	3.5.1	The Successful Bidder will be responsible for supply, installation, maintenance, integration, implementation, support, and management of software-based Web Application Firewall (WAF) solution with warranty, AMC, and Technical Support of the solution at Bank's DC, DR and Near Site for a period of 5 years from the date of go live	This Clause asks for software based WAF for DC, DR & NDR but in technical specification says "The commercial proposal should be based on FQDNs inclusive of unlimited WAF and L3-L7 DDoS (bandwidth) per FQDNS" both the SOW and technical specifications are contadicting.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					Please clarify which solution is NABARD is looking.	
286	Scope of Work and Technical Specifications	1	1.(a)	The RFP seeks to engage a Managed Security Service Provider (MSSP) for providing managed SOC services across the proposed Bank's Infrastructure which consists of Private Cloud spanning across DC, DR and near Site. This includes the procurement of necessary hardware and related tools, as well as the ongoing operations and management of the entire Security solution. The entire solution has to be maintained over a five-year period from the go live date. NABARD may further extend the contract beyond a term of 5 years on a mutual agreement basis	Request for Clarification: As per this clause, does the bidder need to factor in the required Servers, VMs, racks, and servers for all proposed solutions, or will NABARD provide the necessary hardware, VMs, and other components as per the requirements of the proposed solution?	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
287	Scope of Work and Technical Specifications	2	(d)	Integration of components (hardware/software) with each other and the Bank's Infrastructure and with third party devices is the sole responsibility of the selected bidder. Besides, the bidder has to ensure that their tools are integrated in the Bank's / its Cloud provider portals viz., SLA portal, Invoice portal, Service Desk portal, Bird's eye view Dashboard etc.	Request for Clarification: As per this clause, all proposed solutions must be integrated with the tools mentioned. Could you please confirm the exact number of tools involved in this scope along with their names, so we can factor them into our planning? Additionally, if NABARD has any specific use case requirements, kindly share those as well.	Same shall be shared with the successful bidder
288	Scope of Work and Technical Specifications	2	(g)	Online Portal: Integrating into the existing portal provided by the Bank for availability and performance reporting which should be monitored on 24/7 basis	Request for Clarification: Could you please confirm the intended use case here? Is NABARD looking for a unified platform or dashboard that provides end-to-end visibility of the entire SOC, rather than relying separately on individual SIEM or SOAR dashboards?	Kindly refer to the RfP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
289	Scope of Work and Technical Specifications	4	(gg)	Bidder is expected to write parsers, connectors and other programs as necessary to enable integration of all in-scope components and operationalization of the same.	Request for Clarification: Can we propose that up to 10 custom parsers will be developed during the implementation timeline, and post-implementation, additional custom parsers can be created without limitation, based on mutual agreement between the customer and Inspira?	Bidder has to write the parsers as per the requirement of NABARD without any limitation to the timeframe
290	Scope of Work and Technical Specifications	4	(ii)	All the tools proposed by the bidder must be in High Availability mode ensuring redundancy.	Request for Clarification: Could you please confirm the High Availability (HA) setup preference? For example, is it Active in DC and Passive in DR and NDR, or Active with HA in DC, Passive with HA in DR, and Passive with HA in NDR? If there is any other preferred configuration, kindly confirm and specify the same. Additionally, please confirm if all proposed solutions are to be deployed on-premises or	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					NABARD will provide private cloud option as well	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
291	Scope of Work and Technical Specifications	5	3.1.4	Installation and commissioning of adequate log collector at Bank sites (DC, DR and Near Site). Ensure that logs are being collected from all the in-scope devices. As appropriate suggest Bank and related stakeholders on required log-levels and support Bank in enabling the suggested log levels.	Request for Clarification: Could you please confirm the exact architecture expected for the SIEM solution? Can we propose a setup where all log collection components with HA are deployed across DC, DR, and NDR sites, while log processing, console, and other core components are hosted at the bidder's premises in an HA setup? Or is NABARD expecting all SIEM components—including log collectors, processors, and the console—to be deployed with HA at each of the customer's sites (DC, DR, and NDR), with the bidder accessing the SIEM console via a secure VPN tunnel? Additionally, please clarify whether the SIEM should follow an Active setup at DC and Passive at DR and NDR, or if	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					NABARD has a specific architecture preference in mind. A detailed clarification on the desired setup would be greatly appreciated.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
292	Scope of Work and Technical Specifications	6	3.2.7	The Solution (with each of its components) should be configured in High Availability (HA) mode.	Request for Clarification: 1. Could you please confirm the exact architecture expected for the SOAR solution? Can we propose deploying all SOAR components with High Availability (HA) across DC, DR, and NDR sites, or is NABARD expecting an architecture where SOAR components are Active at DC and Passive at DR and NDR? Alternatively, does NABARD have a specific requirement such as Active components at all three sites—DC, DR, and NDR? A detailed clarification on the preferred deployment model would be appreciated. 2. Request for Clarification: Could you please confirm the retention period for online log data for the SOAR solution? Additionally, kindly clarify the	1. Bidder shall propose all the security solutions in HA under active active mode at all the sites. 2. Online logs 6 months . Log archival 5 years.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					archival policy—e.g., 6 months online and 6 months in archival storage.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
293	Scope of Work and Technical Specifications	6	3.2.6	The bidder will be responsible for coordination with the OEM and for completion of the implementation, within the timelines. The bidder shall discuss and finalize the implementation plan in consultation with the Bank's official.	Request for Clarification: Can we propose that the bidder's implementation resources will deploy the proposed products, provided they have proven expertise and relevant experience? We will involve the OEM for a post-deployment health check. Please confirm if this approach will be acceptable.	Kindly refer to the RFP
294	Scope of Work and Technical Specifications	8	3.4.1	The bidder must facilitate threat hunting using hypothesis driven, IOC-driven, analytics-driven methods and situational along with emerging threats.	Request for Clarification: Could you please confirm the frequency of the threat hunting activity? Should it be conducted once every quarter or once every month?	The threat hunting activity shall be performed 24*7 using the proposed SIEM, EDR, TIP, SWG, etc tools.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
295	Scope of Work and Technical Specifications	12	3.8.1	The bidder shall be responsible for supply, implementation, maintenance and support of Attack Surface Monitoring Solution for assets accessible publicly.	Request for Clarification: As per this clause, we have considered all public assets for EASM. For accurate licensing, could you please confirm the following details: 1) Number of Domains 2) Number of VIP Users 3) Number of Public IPs 4) Number of Devices 5) Number of Subdomains 6) Number of Certificates 7) Number of Services	Kindly refer to the RfP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
296	Scope of Work and Technical Specifications	12	3.9.1	The bidder shall be responsible for supply, implementation, maintenance and support of EPP and EDR by providing integrated detection, analysis, and response across the organization's endpoints/servers present in the Bank's Data Centre, Disaster Recovery Centre and Near Site	Request for Clarification: Could you please confirm whether NABARD is looking for a cloud-based EDR or an on-premises EDR solution? If an on-premises EDR is preferred, do we need to propose a High Availability (HA) setup for the management server to ensure coverage of endpoints across both DC and DR? Additionally, within the 500 endpoints, please confirm how many are servers, and whether there are any legacy systems included in the scope.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
297	Scope of Work and Technical Specifications	12	3.9.2	The EPP with EDR solution shall be seamlessly integrated with Bank's existing infrastructure devices and proposed solutions such as AD, SIEM, Firewalls etc. The integration shall be carried out by the bidder	Request for Clariication: As per this clause, we understand that Active Directory (AD), SIEM, and firewall logs need to be integrated with the EDR solution to provide enhanced context for incident management. Kindly confirm if our understanding is correct. If so, please also confirm the number of third-party integrations required, along with the respective OEM details for each.	Please refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
298	Scope of Work and Technical Specifications	12	3.9.6	The EDR solution should meet all the technical/functional specifications of the solution as specified in the Technical Specification sheets.	Request for Clarification: 1) Does the EDR solution need to handle user authentication, or will that be managed by a separate solution? Additionally, can different agents or consoles be used to ensure RFP compliance? 2) Users will authenticate once (SSO) for operating system login, full disk encryption, and other endpoint security modules. In this case, what specific use case is expected from the EDR solution? 3) Should the sandboxing solution be deployed on-premises or in the cloud? 4) Could you please confirm the retention period for online log data if the EDR is hosted on the cloud? Additionally, please clarify the archival policy—for	Please refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					example, 6 months online and 6 months archived	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
299	Scope of Work and Technical Specifications	68	2	The NDR/NBAD tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NDR/NBAD integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.	Request for Clarification: We kindly request the customer to confirm whether we can propose a Software/VM-based NBAD solution. This approach would eliminate the need to manage hardware appliances across multiple locations, resulting in cost savings and simplified resource and hardware planning for the customer. A software-based NBAD deployment is easier to manage and offers the same core functionality as the hardware-based solution, ensuring no compromise on performance or capability. Request for Removal of Clauses Related to NBAD Hardware, appliance and Encrypted Traffic If the customer agrees to adopt a Software/VM-based NBAD	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					solution, we kindly request the NABARD team to remove all clauses from the RFP that refer to NBAD appliances, hardware requirements, and encrypted traffic handling. This will help align the scope with the proposed software-based approach, reduce infrastructure complexity, and streamline solution deployment.	

300	Scope of Work and Technical Specifications	72	73	The solution is capable of performing Encrypted Traffic Analytics to predict with a high level of accuracy whether or not an encrypted flow session is likely to be hiding threat vectors.	Request for Clause Removal: We respectfully request the removal of this clause. As per industry best practices, network traffic decryption is typically handled by a dedicated third-party OEM before the data is ingested into the NBAD solution. Including decryption capabilities within the NBAD scope would significantly increase the overall cost due to the need for additional hardware, licensing, and integration efforts. Furthermore, we recommend that the customer scope the requirement around flow-based traffic ingestion only, rather than a full-fledged NBAD solution. Implementing a complete NBAD setup would require high-performance appliances, extensive hardware, and third-party network traffic decryption tools, all of which will substantially impact the cost. As an alternative, we suggest leveraging flow ingestion with	No change

					multi-device correlation to enable behavior-based detection of abnormal traffic and threats. This approach is cost-effective and still offers robust detection capabilities using flow data and correlation across multiple network and security devices. We strongly recommend deleting this clause to ensure flexibility in solution design and better cost optimization.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
301	Scope of Work and Technical Specifications	13	3.11.1	The bidder shall be responsible for supply, implementation, maintenance and support of NBAD solution across the organization's endpoints/servers present in the Bank's infrastructure.	Request for Clarification: Could you please confirm whether NABARD is specifically looking for an appliance-based architecture, or if the bidder can propose an architecture based on feasibility and best practices? Additionally, please clarify the preferred architecture for the NBAD solution: If the network traffic is the same across DC, DR, and NDR, should the setup be Active at DC and Passive at DR and NDR? If the traffic is distinct across all three sites, should we consider Active at DC, Active at DR, and Active at NDR? Alternatively, do we need to propose Active with HA at DC, Active with HA at DR, and Active with HA at NDR?	Bidder shall propose VM based solutions at NABARD designated locations in HA in active active mode.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					Kindly confirm the expected architecture to help us align our proposal accordingly.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
302	Scope of Work and Technical Specifications	13	3.11.2	The NBAD solution shall be seamlessly integrated with the Bank's existing infrastructure and network devices and the proposed solutions such as AD, SIEM, Firewalls etc. The integration shall be carried out by the bidder.	Request for Clarification: Could you please confirm the expected throughput for the NBAD solution both DC & DR—whether it is 10G, 20G, 30G, or any other specific requirement?	The same shall be shared with the successful bidder.
303	Scope of Work and Technical Specifications	16	6.(a)	Bidder shall arrange the training for all proposed services/ tools by the OEMs proposed as part of the RFP. The topics should cover detailed functionality, configurations, troubleshooting etc of its product.	Request for Clarifications: Could you please confirm the number of participants and the duration of the training? Additionally, please clarify whether we are expected to propose paid certification training or if product-specific training will suffice.	Bidder has to arrange the training for a total of 20-30 NABARD officers. Mode of training may be decided mutually between NABARD and the bidder. Product specification training shall suffice.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
304	Scope of Work and Technical Specifications	64	60	Users will log on one time (SSO) for authentication to the operating system, Full Disk Encryption, and other Endpoint Security blades	Request for Clause Removal: As per this clause, the EDR must have built-in functionality to enable full disk encryption for endpoints. However, in practice, most OEMs rely on third-party products to achieve this functionality, as it is not typically a native feature or specification of an EDR solution. We kindly request NABARD to delete this clause, as full disk encryption is not a standard feature of EDR solutions. This is favouring to Only One OEM	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
305	Scope of Work and Technical Specifications	5	3.1.5	The bidder must provide the bank with read/write access to the SIEM platform	Request for Clause Removal Since This is SOCaaS opportunity where the customer is opting for SIEM as a Service. In this model, due to the nature of MSSP licensing, the bidder cannot provide write access to the end customer on the SIEM platform. However, if the customer requires specific reports for audits or any other purposes, the bidder will generate and provide those reports accordingly. Additionally, in cases where the customer needs to showcase the SIEM platform to a third-party auditor, the SOC team will facilitate appropriate read-only or view access via the online console. In light of this, we respectfully request the removal of this clause, as it does not align with the standard Manages SOC as a	All the tools provisioned as part of the RFP shall be provided on a dedicated basis. However, Resources managing the same may operate remotely in sharing mode.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					service model and licensing constraints.	
306	Scope of Work and Technical Specifications	14	3.12.1	The bidder shall be responsible for supply, implementation, maintenance and support of TIP solution across the organization's endpoints/servers present in the Bank's infrastructure.	Request for Clarification: Is biddeer is expected to provide only threat intelligence feeds, or should we also include the implementation of a full-fledged Threat Intelligence Platform (TIP)? Please clarify	Bidder is expected to provide full fledged TIP solutions with all necessary feeds.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
307	Scope of Work and Technical Specifications	23	3	The Proposed solution should have (Video) learning contents in the console itself.	Request for Clause Removal Justification: Every SIEM platform offers its own unique approach to guiding users through dashboards, building queries, initiating searches, and managing incidents—typically through intuitive graphical user interfaces (GUIs), embedded documentation, tooltips, or integrated help features. However, mandating the presence of in-console video learning content as a requirement may unduly favor a specific OEM, as this is not a standard feature across all platforms. We respectfully request the removal of this clause, as it may create an unequal evaluation environment and limit fair competition among OEMs that provide equally capable but	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					differently designed user guidance mechanisms.	
308	Scope of Work and Technical Specifications	37	102	The solution should incorporate a highly available component architecture to ensure the absence of any single point of failure	we recommend to have HA at Processing layer only to have cost effective solution.Please confirm	NABARD shall provision Virtual Machines over which the bidder has to deploy the security solutions in HA mode in active active at all the locations. Further, all the components shall reside the Private Cloud setup of NABARD.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
309	Scope of Work and Technical Specifications	31	16	The solution should support Active-Active high availability.	Request for Clause Modification: As per industry best practices, an Active-Active High Availability (HA) setup is complex to manage—especially in scenarios involving incident de-duplication across both DC and DR sites. Running all instances in Active-Active mode at both locations significantly increases the overall requirements in terms of hardware, resources, and cost. We recommend modifying this clause to support an Active-Passive HA architecture. This approach is more manageable, cost-effective, and still fully meets the RFP requirements related to availability, architecture, and integrations.	NABARD shall provision Virtual Machines over which the bidder has to deploy the security solutions in HA mode in active active. Further, all the components shall reside the Private Cloud setup of NABARD.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
310	Payment Terms and Conditions	1	3	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 10% cost of the monthly contracted amount. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the monthly contracted amount even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 5% cost of the monthly contracted amount. However, Penalty under individual towers shall be added and overall penalty in this case may not go above 10% of the monthly contracted amount even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor	Kindly refer to corrigendum
311	Payment Terms and Conditions	1	2	Payment shall be made on a quarterly basis, in arrears.	Payment shall be made on a Monthly basis, in arrears. As Invoices are expected to be raised on monthly basis.	No change
312	General			Additional Point	kindly confirm can we propose shared model for the tools.	Bidder has to provide tools on a dedicated basis. However, the resources

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
						provided can be on shared basis.
313	Payment Terms and Conditions	1	2	kindly change the payment terms as annual advance since we have to buy the tools(DAM, WAF, NBAD, EDR,Proxy,PAM,SCM,EASM) from the OEM upfrontly and have to pay upfrontly to the OEM.	kindly change the payment terms as annual advance	No change
314	Payment Terms and Conditions	1	2	All this OEMare not ready for quatelrly payment so kindly change the payment terms to yearly advance.	All this OEMare not ready for quatelrly payment so kindly change the payment terms to yearly advance.	No Change
315	General			Additional Point	Can we propose cloud based solution also because there are some solutions which comes in cloud format only. (EASM and proxy are cloudbased solution) Kindly confrim on the if we can propose cloudbased solutions	Bidder may propose Cloud based EASM solution if on prem solution is not feasible.
316	GeM Bid Document			PBG	Bank Guarantee (PGB) for an amount of 5% of the total annual value order of works	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
130	Scope of Work and Technical Specifications	65	79	The anti-ransomware solution has third party-validation	Request to share more details on Third party validation	Same shall be shared with successful bidder.

318	Scope of Work and Technical Specifications	24	41	High Availability should use cluster set-up so that data could be shared between the nodes.	Request for Clause Removal: Justification: Most SIEM solutions consist of core components such as log collectors, processors, and consoles—although terminology may differ across OEMs. These components are typically deployed in a High Availability (HA) configuration to ensure resilience, fault tolerance, and continuous operations. Mandating a cluster-based architecture for all components would significantly increase the infrastructure footprint, including hardware, storage, CPU, and supporting components. It would also require load balancers at every level—from collection to processing to presentation—which would lead to higher commercial implications for both the customer and the bidder. We recommend removing this clause and allowing the bidder to propose all essential SIEM components in High Availability	Kindly refer to corrigendum

					mode as per industry best practices and platform capabilities. This approach will meet the functional requirements without unnecessary architectural overhead or cost inflation. Furthermore, this clause appears to favor a specific OEM that uses cluster-based by design, thereby limiting fair competition.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
319	BOM and Commercials	1	3	WAF as a Service - 300 mbps	Please provide details of your applications : 1. are these applications hosted in on-premise (DC, DR & NDR) which needs to be protected, or 2. the applications hosted in cloud (ex., AWS, GCP, Azure, OCP) to be protected using WAAP as a service. These licenses will be based on number of FQDN	1. The applications are hosted in the Private Cloud of NABARD. 2. The licenses should be provided on the basis of throughput
320	Scope of Work and Technical Specifications	33	40	The solution should support sending out authenticated surveys to drive the investigation workflow.	Request you to relax this clause / requirement.	No change
321	Scope of Work and Technical Specifications	34	62	The solution should use machine learning for analyst assignments and auto-calculate incident severity	Request you to modify the given clause / requirement to the following. Solution should have capability for automatic analyst assignment and calculate incident severity.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
322	Scope of Work and Technical Specifications	34	63	The solution should support the creation of customizable forms for change/request management.	Request you to modify the given clause / requirement to the following. Solution should support creation of HTML forms for change/request management.	No change
323	Scope of Work and Technical Specifications	37	104	The vendor needs to be responsible for ensuring that the implemented solution complies with the specifications detailed in ISO 27001, ISO 27002, RBI, PCI DSS, CERT-IN, IT ACT 2000, DPDP 2023, etc. and any other law of the land applicable for NABARD.	Request you to relax this clause / requirement or NABARD to provide necessary information on standards, frameworks, directives, guidelines and requirements for compliance / adherence to its respective specifications.	No change
324	Scope of Work and Technical Specifications	38	5	Proposed WAAP Solution should have direct API integration with AWS, GCP, AZURE - to attach its VPC/VNETs with SaaS Network privately.	Request you to provide more details and clarity against the mentioned clause / requirement.	Kindly refer to the RFP
325	Scope of Work and Technical Specifications	38	7	The proposed WAAP solution should support SSO for access management using OKTA, Google, Azure AD	Request you to provide more details and clarity against the mentioned clause / requirement.	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
326	Service Level Agreement	8	4.2.2	The Service Provider shall submit monthly reports on the 05th day of each calendar month to NABARD, with such details and in the format, as may be mutually agreed between the Parties, specifying compliance with the Service Levels.	Considering a shared service & support delivery model, request you to consider monthly reports on 15th day of each calendar month instead.	No change
327	Service Level Agreement	8	4.3	4.3. Adherence to RBI directions, guidelines The service provider shall strictly adhere to all directions issued by the Reserve Bank of India (RBI) in relation to the activities outsourced to the service provider by NABARD. The service provider shall regularly monitor and update its internal processes, policies, and procedures to ensure compliance with the latest directives and guidelines provided by RBI. Any modifications required to align with RBI directives shall be promptly implemented by the service	Considering a shared service & support delivery model, request you to relax these clauses / requirements.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				provider to maintain compliance.		
328	Service Level Agreement	9	5.7	Service Provider will sign agreements with OEMs for any support services required from them and shall be responsible for any SLA in this regard, which shall be agreed between NABARD and Service Provider.	While the service provider will have OEM agreement for the support services, request you to relax the requirement of SLA responsibility with the OEM.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
329	Service Level Agreement	10	7.2	The Service Provider shall appoint sufficient number of individuals in order to ensure that the Support Services are provided to NABARD in a proper, timely and efficient manner. The Service Provider shall provide NABARD with the names of the individuals who shall be involved in carrying out the Support Services and shall obtain approval in writing from NABARD before making any change in such team. The individuals appointed by the Service Provider shall be those indicated by the Service Provider under its response to the RFP/GeM Bid. Any additional individual shall be appointed subject to prior written approval from NABARD	Considering a shared service & support delivery model, request you to relax these clauses / requirements.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
330	Service Level Agreement	11	7.4	The Service Provider shall maintain electronic books of accounts, log-books and any other operating records that it may deem necessary in connection with the rendering of Support Services under this Agreement. The Service Provider shall retain all such electronic books of accounts and operating records relating to the Support Services for a period of 7 (seven) years after the expiry or earlier termination of the Agreement.	Considering a shared multi-tenant service & support delivery model, request you to relax this clause / requirement.	No change
331	Service Level Agreement	13	10.1	Service Provider to offer training to NABARD's employees as defined in the RFP/GeM Bid on the software/hardware covering features, facilities, operations, implementation, trouble shooting, system administration, audit, MIS including report generation, etc.	Please let us know the no. of employees, the no. of days and the tools / solutions / technologies for which training needs to be provided to NABARD employees.	Bidder has to arrange the training for a total of 20-30 NABARD officers. Mode of training may be decided mutually between NABARD and the bidder. Product specification training shall suffice.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
332	Service Level Agreement	13	10.4	Training - While On-site training is the norm, web-based training could also be considered keeping in view exigencies as decided mutually. Where Web based training is provided, on-site training could be considered at a later point. Online and offline content also to be part of Training set up and knowledge transfer. Simple and easy to understand short videos on various features, wherever needed; functionalities and workflows may be designed as ready reckoner to further accelerate the training process. SERVICE PROVIDER may need to coordinate and provide content for the development of e-learning modules of NABARD.	Since the service provider might not possess expertise on NABARD's tools, processes etc., request you to relax the requirement of development of e-learning modules.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
333	Service Level Agreement	15	14.2	Bank regularly undertakes periodic checks and VAPT exercises to identify any vulnerabilities in the system. The Service Provider shall make suitable changes as per the recommendations emerging from VAPTs emerging within the contract period. The vulnerabilities so identified may be fixed by the Service Provider within the predefined timeline as follows: A. All Critical & High category Vulnerabilities – To be fixed at the earliest with highest priority and within 1 working day of informing. B. All Medium Category Vulnerabilities – Within 3 working days of informing C. All Other category vulnerabilities – Within 5 working days of informing	Considering a shared service & support delivery model, request you to consider fixing of vulnerabilities based on mutual discussion & agreement between service provider & NABARD in place of the given timelines.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
334	Service Level Agreement	32	1.1.7	Root cause analysis (RCA) should be prepared for all cases of breach in SLA's and shared with NABARD. For any exceptions or SLA breach beyond the control of the selected bidder, the service provider may submit the RCA along with a justification, which may be considered by NABARD. In case the RCA establishes that the breach on SLA was on account of infrastructure issues, the service provider would be liable for the applicable penalty.	Request you to consider necessary explanation over email for SLA breach in place of RCA.	No change
335	Service Level Agreement	32	1.1.9	The service provider should use the tool provided by the NLDR service provider and do an integrated monitoring of the entire IT security setup at Data Center, DR site, near site. Dashboard customization and reporting to be done in consultation with NABARD.	Request you to consider leveraging SOC service provider's tool for monitoring of IT Security setup in place of NLDR service provider's tool owing to technical constraints, compatibility / feasibility challenges, additional commercials involvement etc.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
336	Service Level Agreement	32	1.1.10	The service provider needs to carry out real-time monitoring as well as reporting of SLA parameters and will also be required to provide an integrated and automated monitoring report to NABARD on monthly basis, or as requested by NABARD. All SLAs to the extent possible should be monitored through the automated tools provided by bidder	Request you to consider manual SLA report to be generated by the service provider in place of automated monitoring report to NABARD on monthly basis or as per request. Also request you to consider SLA monitoring via manual methods in place of automated tools.	No change
337	Service Level Agreement	33	1.1.12	SLA treatment shall be based on the root cause analysis and accordingly the SLA treatment shall be given to the ticket for the issue.	Request you to consider SLA treatment based on impact & severity in place of root cause analysis (RCA), as RCA is carried out post incident / ticket generation.	No change
338	Service Level Agreement	33	1.1.13	Completion of the project shall happen in the stipulated timeline as given in the Timelines and Deliverables document.	Request you to consider the suggested changes (as mentioned subsequently) for the timelines based on the respective sections & aspects of the Timelines & Deliverables document.	No change
339	Service Level Agreement	33	1.1.14	The responsibility of coordination with multiple teams/OEMs and	Considering a shared service & support delivery model, request	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				other stakeholders shall lie with the service provider.	you to relax this clause / requirement.	
340	Service Level Agreement	33	1.1.16	Comprehensive onsite support as mentioned in the scope of work under this project.	Please advise if the resource support model needs to be completely onsite or can be hybrid with resources deployed remotely in addition to onsite. Also please share across the location details for onsite resources.	Resources managing the entire setup can provide the services remotely.
341	Service Level Agreement	33	1.1.21.1.(b)	Provision, maintain and use adequate and auditable tools and procedures so as to be able to fully perform all of its obligations under this Schedule, including a Service Level monitoring tool and other tools that: § automatically monitors Service Levels in real time and provides automated reports; § can be accessed by NABARD in real time through a consolidated dashboard;, § provides automated status issues at each layer of Customer infrastructure, network, and applications; and	Request you to consider manual SLA reports in place of automated reports and exclude service level monitoring in real-time via consolidated dashboard.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				§ record all data created as part of its monitoring or measurement activities or otherwise in connection with the performance of the Services,		
342	Service Level Agreement	33	1.1.21.2	On fifth (5) day of each calendar month, service provider shall provide NABARD with a written (paper or electronic) monthly report detailing the actual levels performance of the Solution, the O&M Services, and the Services against the Service Levels and KPIs in such month, together with:	Considering a shared service & support delivery model, request you to consider 15th day of each calendar month instead.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
343	Project Timelines and Deliverables	1	1 and 2	Procure and supply solution components at DC, DR & Near site - T + 1 Months Installation, configuration and commissioning of the tools - T + 45 Days	Considering involvement of multiple tools/solutions across DC, DR & near sites, request you to consider the following timelines instead. 1) T + 60 Days 2) T + 150 Days	No change
344	Project Timelines and Deliverables	1	D1	Detailed Project Plan and inception report- M1	Considering involvement of multiple tools/solutions across DC, DR & near sites, request you to consider due date for the given deliverable to be M1 + 15 days	No change
345	Project Timelines and Deliverables	1	D2	System Design Document (SDD)- M1	Considering involvement of multiple tools/solutions across DC, DR & near sites, request you to consider due date for the given deliverable to be M1 + 30 days	No change
346	Project Timelines and Deliverables	2	D3	Security Tools procurement configuration & implementation- M1	Considering involvement of multiple tools/solutions across DC, DR & near sites, request you to consider due date for the given deliverable to be M1 + 120 days	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
347	Project Timelines and Deliverables	2	D4	User acceptance testing- M1	Considering involvement of multiple tools/solutions across DC, DR & near sites, request you to consider due date for the given deliverable to be M1 + 135 days	No change
348	Project Timelines and Deliverables	2	D5	Go-live	Considering involvement of multiple tools/solutions across DC, DR & near sites, request you to consider due date for the given deliverable to be M1 + 150 days	No change
349	Service Level Agreement	37	3	All the SLAs must be managed by the vendor. Any gap between RFP SLA and SLA provided by respective OEM of the IT infrastructure and other components shall be managed by the vendor with no impact on the client.	Request you to relax this requirement of back-to-back SLA between service provider and OEM.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
350	Scope of Work and Technical Specifications	1 and 3	1. (a) and 2.(j)	The RFP seeks to engage a Managed Security Service Provider (MSSP) for providing managed SOC services across the proposed Bank's Infrastructure which consists of Private Cloud spanning across DC, DR and near Site. This includes the procurement of necessary hardware and related tools, as well as the ongoing operations and management of the entire Security solution. The entire solution has to be maintained over a five-year period from the go live date. NABARD may further extend the contract beyond a term of 5 years on a mutual agreement basis.	1. Please let us know whether multi-tenant shared platform based security service, support, operations / delivery is acceptable or bidder needs to provision dedicated setup and resources for NABARD. Also please share across the location and region of DC, DR and Near sites as well as NABARD offices. 2. Since the security solutions need to be deployed within Bank's DC, DR & Near sites within Ctrl-S Data centers, requesting bank or its infra partner to provision/deploy necessary hardware/ infra (CPU, RAM, storage) & network connectivity requirements while the application, software, licenses will be catered to by the SOC service provider.	1. Dedicated setup is expected. 2. NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
351	Scope of Work and Technical Specifications	1	2.(a)	The bidder must deliver managed security services for NABARD, ensuring that the entire solution is deployed at NABARD designated locations on pay-as-you-go model. This approach aims to ensure that NABARD's infrastructure is both secure and scalable, meeting the organization's evolving needs over the contract period	Please suggest if its fine to consider SaaS based solutions (public cloud / Hyperscaler based) in place of each of the solutions deployed at NABARD designated locations as certain solutions (For e.g. TIP, EASM) are provided by OEM's only in a SaaS model.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.
352	Scope of Work and Technical Specifications	1	2.(b)	The solution shall include Supply, Installation, Implementation, Integration, Roll Out, Operations and Maintenance of all the security tools listed in this RFP in DC, DR and Near site for the entire contract duration:	Please let us know whether implementation needs to be carried out onsite or can be done remotely with necessary hands & feet, racking, stacking, remote access etc. support provided from NABARD end. In case of onsite implementation, please let us know the exact location &	Bidder may carry out the implementation and support remotely. However, they need to ensure that the timelines are strictly met

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					address of the facilities for implementation.	
353	Scope of Work and Technical Specifications	1	2. (d)	Integration of components (hardware/software) with each other and the Bank's Infrastructure and with third party devices is the sole responsibility of the selected bidder. Besides, the bidder has to ensure that their tools are integrated in the Bank's / its Cloud provider portals viz., SLA portal, Invoice portal, Service Desk portal, Bird's eye view Dashboard etc.	1. Considering a shared service & support delivery model, request you to consider integration of Bank's infrastructure to be carried out by Bank's in-house infra-team or infra partner / vendor accordingly. 2. Request you to consider utilization of bidder's own tools / solutions / portals in place of Bank's / its Cloud provider portals.	Kindly refer to the RFP
354	Scope of Work and Technical Specifications	1	2.(g)	Online Portal: Integrating into the existing portal provided by the Bank for availability and performance reporting which should be monitored on 24/7 basis.	Request you to consider utilization of bidder's own tools / solutions / portals in place of existing portal provided by the bank.	In addition to the dashboard provided by the bidder the same shall be integrated with the bank's Online portal.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
355	Scope of Work and Technical Specifications	3	2.(m)	The entire solution shall be scalable at short notice within 1 month of the request from NABARD and shall be governed by SLA.	Owing to dependencies like technical feasibility, change management processes, business & technical approval from NABARD end etc. reqquest you to consider solution scalability timeline based on mutual discussion & agreement between NABARD & service provider.	No Change
356	Scope of Work and Technical Specifications	3	(w)	All tools supplied as part of the project should undergo annual health checkup by the respective OEMs and the certificate for same should be submitted to NABARD.	Request you to relax this clause / requirement or consider annual health checkup by the service provider with email confirmation in place of activity to be carried out by the OEM along with certificate submission.	No change
357	Scope of Work and Technical Specifications	4	(y)	Licenses for the entire project may be procured in the name of the vendor or NABARD. However, any such arrangements should not violate the licensing policy of any OEM. The service provider shall be liable for any punitive action or damage for violation of licensing policies.	Since the solution & support needs to be in an Opex model, please clarify whether the licenses needs to be in NABARD's name or service provider's name.	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
358	Scope of Work and Technical Specifications	4	(dd)	Bidder will facilitate Bank to assess SOC functioning, including all physical facilities involved in service delivery, such as the SOC and areas where client data is stored / processed periodically. Monthly/periodic visits will be facilitated by the bidder to SOC premises where bank authorities can come, visit the SOC and meet with the resources hired for the project. The Staff hired can be called to bank premises in Bank's HO whenever required by Bank officials. All expenditure pertaining to this must be borne by the bidder.	Considering a shared service & support delivery model, request you to relax this clause / requirement.	No Change
359	Scope of Work and Technical Specifications	4	(ee)	Bank will have complete oversight and ownership over the rule definition, customization and related data/ logs, meta-data and analytics related to SOC services	Request you to relax this clause / requirement as it can lead to dual ownership issues between the bank & the service provider.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
360	Scope of Work and Technical Specifications	4	(hh)	Technical Specifications of all the tools mentioned below are detailed in the Technical Specification Sheet. At the end of the implementation, the bidder has to arrange for a Certificate from the respective OEMs, certifying that the implementation deployed solution meets all the technical/functional specifications of the solution as specified in Technical Specifications in this RFP.	Request you to relax this clause / requirement or consider review and recommendation from respective OEMs at the end of implementation in place of providing a certificate from the respective OEM.	No Change
361	Scope of Work and Technical Specifications	5	(nn)	The Solution deployed as part of the RfP shall not be extended to any 3rd party	Request you to relax this clause / requirement or clarify whether sub-contracting is allowed or not.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
362	Scope of Work and Technical Specifications	5	(pp)	The bidder must provide an initial notification within 24 hours of identifying a breach or security incident, with a detailed incident report to be submitted within 72 hours, covering: · Nature and scope of the incident · Systems/data affected · Mitigation steps undertaken · Impact analysis · Preventive actions for future	Request you to consider timelines for detailed incident report to be decided based on mutual discussion & agreement between NABARD and the service provider on a case-to-case basis depending on the nature of the incident, its impact, its severity etc. in place of the mentioned 72 Hours.	No change
363	Scope of Work and Technical Specifications	5	3.1.1	The SIEM solution shall seamlessly integrate with Bank's existing infrastructure devices like servers, switches, routers, SDWAN, DB, Applications, AD, Email gateway, firewall devices, backup devices etc and proposed security solutions of the RFP such as SOAR, PAM, DAM, WAF, AV, EDR, etc	For effective SIEM, sizing & solutioning and parser, integration method considerations, request you to share across a break-up of devices/log sources with quantity/count, Make & Model, Operating system info with version no., deployment type (on-prem/SaaS), device-type (physical/virtual), no. of users across DC, DR, Near Site, Head-Office, Branch/Remote-Office locations, cloud environments (e.g. AWS, Azure, GCP etc.) along with the type of network connectivity (e.g. Site-to-Site	Same shall be shared with the successfule bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					VPN, MPLS, P2P, AWS Direct-Connect, Azure Express Route etc.) between each of these locations/environments.	
364	Scope of Work and Technical Specifications	5	3.1.4	Installation and commissioning of adequate log collector at Bank sites (DC, DR and Near Site). Ensure that logs are being collected from all the in-scope devices. As appropriate suggest Bank and related stakeholders on required log-levels and support Bank in enabling the suggested log levels	It is being understood that the necessary hardware / infra for the provisioning of the log collectors would be taken care by the bank or its Data center service provider. Please advise if otherwise.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
						active-active mode at all the sites.
365	Scope of Work and Technical Specifications	6	3.1.7	The SIEM solution must provide User Behavior Analytics capabilities as detailed in technical specifications	For UBA functionality, please share across the total number of your organization users who have accounts either in AD/VPN/Proxy & so on.	The same shall be shared with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
366	Scope of Work and Technical Specifications	6	3.1.8	The bidder to share the above-mentioned reports with Bank: a. Use cases implemented (Weekly) b. Use cases triggered (Realtime) c. Log sources not triggering (Realtime) d. Utilization report in EPS (Weekly) e. Incident report (Daily, Weekly and Monthly) f. SIEM Inventory (Weekly)	Request you to consider email notifications in place of reports for the following and within mutually agreed timelines in place of real-time or near real-time. b. Use cases triggered c. Log sources not triggering e. Incident report	No change
367	Scope of Work and Technical Specifications	6	3.2.1	The MSSP Bidder shall be responsible for supply, implementation, maintenance and support of SOAR Solution at Bank's infrastruc	Please assist with the following inputs for SOAR sizing & solutioning. a) No. of SOAR user licenses b) No. of playbooks to be configured c) No. of incidents / alerts per day c) Whether uni-directional or bi-directional integration is needed with in-scope solutions like SIEM, NBAD, TIP, WAF, DAM, PAM, EDR, SWG etc .	Please refer to BOM and Commercials. Further details shall be shared with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
368	Scope of Work and Technical Specifications	6	3.2.3	In case there is a requirement of the integration of SOAR solution with any existing or new security device/solution within the contract period, the same is to be done by the bidder without any cost to the Bank	Since integration of new security device / solution can involve additional commercials, request you to relax this clause / requirement of without any cost to the Bank.	No change
369	Scope of Work and Technical Specifications	7	3.3.4	Bidder shall coordinate with other departments/teams/vendors for mitigation and closure of the incident.	Considering a shared service & support delivery model, request you to relax this clause / requirement.	No change
370	Scope of Work and Technical Specifications	8	3.3.10	The bidder shall be responsible for Reporting and logging of information security incidents through the use of Bank's ticketing tool.	Considering a shared service & support delivery model, request you to consider leveraging the SOC service provider's ticketing tool instead. If not, request you to provide the make & model of the Bank's ticketing tool and it's deployment type on-prem or SaaS for solution design accordingly.	Kindly refer to the RfP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
371	Scope of Work and Technical Specifications	10	3.5.5	The minimum application throughput WAF must be 300 Mbps	Please assist with the following inputs for WAF sizing & solutioning. a) No. of Requests b) Count & details of URL's /FQDN's wth port nos to be protected behind WAF c) L3/L4 DDoS --> Do we consider separate or only for FQDNs onboarded d) Current Websites Domains DNS hosting provider name e) Also does the current Domains DNS hosting provider support DNS CNAME Flattening ?	Bidder to provide the WAF Solution on Through put basis and not on the number of FQDN.
372	Scope of Work and Technical Specifications	10	3.5.10	In case there is a requirement of integration of WAF solution with any existing or new security device/solution, within the contract period the same is to be done by the bidder without any cost to the Bank	Since integration of new security device / solution can involve additional commercials, request you to relax this clause / requirement of without any cost to the Bank.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
373	Scope of Work and Technical Specifications	11	3.6.1	The bidder shall be responsible for supply, implementation, maintenance and support of Database Activity Monitoring for 80 Database Servers across DC, DR and Near Site	Please assist with the following inputs for DAM sizing & solutioning. a) Details of Database technology (MSSQL, Oracle, MYSQL, Cloud DBaaS etc.) in scope b) Database Server Count/Inventory details along with CPU cores count and Active/Passive details for each of the DB Servers c) Size of DB Logs Per Database Per Day in MB / GB	The same shall be shared with the successful bidder.
374	Scope of Work and Technical Specifications	11	3.7.1	The bidder shall be responsible for supply, implementation, maintenance and support of PAM Solution for endpoints/servers present in Bank's infrastructure	Please assist with the following inputs for PAM sizing & solutioning. a) No. of Users that will have access b) No. of Devices that will be integrated	Kindly refer to the BOM and Commercials

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
375	Scope of Work and Technical Specifications	12	3.8.1	The bidder shall be responsible for supply, implementation, maintenance and support of Attack Surface Monitoring Solution for assets accessible publicly	Please assist with the following inputs for EASM sizing & solutioning. a) No. of Public facing IP's & domains b) No. of web & email domains c) No. of mobile applications with type (Android / IOS) d) No. of takedowns e) No. of key executives to be monitored f) No. of social media accounts / handles g) No. of keywords & brand names h) No. of paste-bin sites / URL's	Please refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
376	Scope of Work and Technical Specifications	12	3.9.1	The bidder shall be responsible for supply, implementation, maintenance and support of EPP and EDR by providing integrated detection, analysis, and response across the organization's endpoints/servers present in the Bank's Data Centre, Disaster Recovery Centre and Near Site.	Please assist with the following inputs for EPP, EDR sizing & solutioning. a) No of User Workstations, Servers / Endpoints b) OS Version (Linux kernel versions, Windows 7/ 8 / 10, MAC, Windows 2016/2019…) deployed on the Endpoints / Servers c) Inventory split of nos. of Servers and Desktop/Laptop Endpoints d) In case of Cloud Service, if Containers/Kubernetes to be covered under EDR Service, please provide its count.	Please refer to the RFP
377	Scope of Work and Technical Specifications	13	3.10.4	The solution should be deployed at 500 endpoints (OS included)	Please let us know if the 500 endpoints count is inclusive of servers or only limited to end user systems like desktops, laptops and workstations. Request you to share across a breakup of servers and end user systems for more visibility and effective solution design & sizing.	All the endpoints mentioned in the RFP are for servers only.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
378	Scope of Work and Technical Specifications	13	3.11.1	The bidder shall be responsible for supply, implementation, maintenance and support of NBAD solution across the organization's endpoints/servers present in the Bank's infrastructure	Please assist with the following inputs for NBAD sizing & solutioning. Count of Servers & count of workstations seperately within the infra with its breakup across DC , DR & NDR , Branch / Remote office locations & Cloud environments.	The same shall be shared with the successful bidder.
379	Scope of Work and Technical Specifications	14	3.13.1	The bidder shall be responsible for supply, implementation, maintenance and support of SCM solution across the organization's endpoints/servers present in the Bank's infrastructure.	Please assist with the following inputs for solution design & sizing. 1. Does the bank intend to perform CIS benchmarking checks, or are they looking to run custom audit file checks? 2. If custom audit files are required, could you please confirm the number of checks included in each file? 3. Please share across the exact list of controls to be covered. 4. Please share the list of target devices, along with the operating system versions, as CIS controls vary based on OS	The same shall be shared with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					versions. 5. Please share across the total assets count to derive the commercial proposal.	
380	Scope of Work and Technical Specifications	16	8.(a)	NABARD will review and discuss the performance during the first week of every month	Request you to consider a timeframe for review & performance discussion based on mutual discussion & agreement between the service provider & NABARD in place of during first week of every month.	No change
381	Scope of Work and Technical Specifications	16	8.(d)	All review meetings will be held at NABARD's designated site.	Request you to consider remote / virtual meetings in place of NABARD's designated site considering a shared service & support delivery model.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
382	Scope of Work and Technical Specifications	19	11	The bidder shall provide all necessary support for completing all migration and transfer activities, either during the project or before the contract's termination. This includes transitioning to any alternative setup, such as public, private, hybrid, or government cloud solutions. Additionally, the bidder shall also provide full support for the migration of the current security solutions to the proposed setup.	Migration / transfer activities during the project or prior to contract termination as well as to alternative setup like public, private, hybrid, or government cloud solutions would be subject to technical feasibility, fulfilment of pre-requisites & approval from NABARD end as well as involvement of additional commercials if applicable. Hoping this is acceptable.	Please refer to the RFP

383	QCBS Evaluation Criteria	###	B.(2)	(A) The proposed SIEM solution with a minimum of 10000 EPS should have been supplied and implemented by OEM in India in last five years (B) The proposed SOAR + TIP solution with should have been supplied and implemented by OEM in India in last five years (C) The proposed WAF solution with should have been supplied and implemented by OEM in India in last five years (D) The proposed DAM solution with should have been supplied and implemented by OEM in India in last five years (E) The proposed SWG solution with should have been supplied and implemented by OEM in India in last five years (F) The proposed PAM solution with should have been supplied and implemented by OEM in India in last five years (G) The proposed EDR solution with should have been supplied	1. Request you to consider any OEM based SIEM, SOAR, TIP, WAF, DAM, SWG, PAM, EDR, EASM, SCM, NBAD solutions (not limited to proposed) supplied & implemented by the SOC service provider in place of by the OEM. 2. Request you to consider SOC service provider in place of the OEM for the mentioned clause / requirement.	Kindly refer to corrigendum

				and implemented by OEM in India in last five years (H) The proposed EASM solution with should have been supplied and implemented by OEM in India in last five years (I) The proposed SCM solution with should have been supplied and implemented by OEM in India in last five years (J) The proposed NBAD solution with should have been supplied and implemented by OEM in India in last five years OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices/signoff Letter.		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
384	QCBS Evaluation Criteria	4	C	Scoring Criteria for bidder Certifications: a. ISO27001 Certification - 2 Marks b. Cert-in Empanelment - 2 Marks c. SOC II Type II Certification - 1 Marks All these certifications should be valid as on 1st April 2025.	Request you to relax the requirement of Cert-In Empanelment from the mentioned criteria.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
385	QCBS Evaluation Criteria	4	D	The bidder must have IT Security resources on permanent payroll having experience in-scope solutions with Certifications such as CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) 50 to 75 resources- 04 marks (b) 76 and above resources- 09 marks Note: (i) Resources for CEH- Max 10 resources will be considered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource has more than one certification, it will be considered as one. (iii) Of the above, the bidder must have a total of 5 certified resources of the proposed SIEM solution on permanent payroll. If not, then the count of resources will not be considered, and no marks shall be awarded under Clause'D'.	i) Request you to consider candidates with other certifications as well in place of the given list. ii) Request you to consider CEH certified resource count to be greater than 10. iii) Request you to relax the requirement of total 5 certified resources of the proposed SIEM solution.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
386	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH certified. Note: (i) Resources for CEHMax 10 resources shall be considered. The certification date must be prior to the date of	i) Request you to consider candidates with other certifications as well in place of the given list. ii) Request you to consider CEH certified resource count to be greater than 10.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				publication of this RFP. (ii) If a resource is carrying more than one certification, it shall be considered as one.		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
387	Minimum Eligibility Criteria	4	3	The bidder must fulfil the above eligibility criteria conditions. Bids not complying with any of the eligibility criteria are liable to be rejected and will not be considered for further evaluation.	Request you to consider bids fulfiling the eligibility criteria partially in order to provide a fare chance and allow multiple bidders to participate.	No change
388	General			Additional Point	a) Is NABARD looking at Cloud Native vendors. b) Is NABARD fine to deploy client on end user devices and send via Cloud Native solution for end users.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.
389	General			Additional Point	Is NABARD looking at Web DLP controls with advance DLP controls like OCR and AI/ML capabilities from Cloud Native vendor.	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
390	General	40	4	Secure Web Gateway (SWG) /Web Proxy Additional Point	Request you to consider the following requirement as well as part of SWG. The solution must have inbuilt Incident Management for DLP Events. The Management console such assist DLP admin to quickly take informed decision by looking at snip highlighting content of the policy violations as well as download Original File incidents.	No change
391	General	40	4	Secure Web Gateway (SWG) /Web Proxy Additional Point	Request you to consider the following requirement as well as part of SWG. The solution must support 20+ compliance templates along with predefined India PII data classifiers, Aadhar, Indian PAN, Indian Names (First Name, Last Name), Photo ID (India Passport, India Driving License) etc. to ensure necessary compliances.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
392	General	40	4	Secure Web Gateway (SWG) /Web Proxy Additional Point	Request you to consider the following requirement as well as part of SWG. Solution should utilize AI and machine learning or behavior analysis / sandboxing to detect and block malicious portable (PE) files from any URL category, with the ability to prevent Zero Day Attack.	No change
393	General	40	4	Secure Web Gateway (SWG) /Web Proxy Additional Point	Request you to consider the following requirement as well as part of SWG. The vendor must provide SLA for decrypted traffic, committing to less than or ~ 60 ms to 125 ms latency for processing encrypted traffic to ensure better performance while accessing applications and better end user experience.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
394	Service Level Agreement	18	18	Limitation of Liability	It is hereby submitted that the Limitation of Liability clause is in conflict with the GeM terms. As per GeM terms both parties liability is limited. However as per the SLA document the Limitation of Liability is applicable only for SLA breaches. It is hereby submitted that the GeM terms on limiting liability as reproduced below should be added to the Limitation of Liability clause: In any event, neither party shall be liable for any special, incidental, punitive, exemplary or consequential damages arising out of or in connection with the Contract entered between the parties. The aggregate liability of either party, whether under the contract, in tort or otherwise, shall not exceed the total contract value, provided that this limitation shall not apply to:	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					(i) Any obligation or claim arising out of or in connection with any third party claim of IPR infringement, (ii) In the event of any gross negligence or willful misconduct on part of either party, as finally judicially determined by a court of competent jurisdiction.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
395	Service Level Agreement	22	22	Indemnification	Indemnity under 22.1.1 shall be deleted. There shouldn't be a generic Indemnity on Breach of the Terms of the Agreement. The Agreement particularly includes terms like SLA etc. also. For which separate remedies like SLA credits are available. Hence this generic Indemnity shall be deleted. For this breach the route of suing the other party for breach of contract is anyways available. Clause 22.3 further states that The rights of NABARD pursuant to this Clause (Indemnification) shall be in addition to and not exclusive of, and shall be without prejudice to, any other rights and remedies available to NABARD at equity or Law including the right to seek specific performance, rescission, restitution or other injunctive relief, none of which rights or remedies shall be affected or diminished thereby.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					It is highly onerous on the Bidder that for Service Level issues Client will claim SLA credits and indemnities for the same breaches also.	
396	General			Additional Point	Current ITSM tool and hope we can integrate it with our tool if remote shared model is being considered. Also, assumptions are that first level ticket triaging will be done by NABARD existing helpdesk team	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
397	General			Additional Point	There are some places(SLA PDF) where customer is allowing to subcontract with intimation to NABARD but in some placed, they are asking for NTT payroll staff. Need clarity	Kindly refer to the RfP
398	Service Level Agreement	39	3.3.1	NABARD will levy penalty if 100% of the system is not in n-1 version starting from patch/update release date	Request to change it as we will do patch and updates in UAT first and if it is successful then only will be moved to production.	No change
399	Payment Terms and Conditions	1	2	Payment shall be made on a quarterly basis, in arrears.	Request to change the payment term to Quarterly in advance	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
400	Payment Terms and Conditions	1	3	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 10% cost of the monthly contracted amount. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the monthly contracted amount even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 3% cost of the monthlycontracted amount. However, Penalty under individual towers shall be addedand overall penalty in this case may go above 3% of the monthly contractedamount even though the penalty under individual tower shall be restricted to 5 %. In addition to the penalty, proportionate payment for the downtimeexcept for approved downtime shall not be made to the vendo	Kindly refer to corrigendum

401	Service Level Agreement	23	23.2.1	Order Cancellation/ Termination of Contract NABARD reserves its right to cancel the entire/ unexecuted part of Purchase Order at any time by without assigning appropriate reasons in the event of one or more of the following conditions: a. Delay in Implementation of the Project beyond the specified periods for reasons solely ascribed to the Service Provider. b. Serious discrepancies noted in the implementation of the project. c. Breaches in the terms and conditions of the Purchase Order. d. Project adversely affecting the Core Systems or Core Business of the NABARD and the normal functioning of the Offices of NABARD. e. If Service Provider fails to upgrade any or all of the critical hardware /software within the period(s) specified in the Contract or within any extension thereof granted by the NABARD. f. If Service Provider fails to perform any other obligation(s) under the Contract. g. If Service Provider is not providing after sales and maintenance services and the calls	Termination for convenience is subject to 90 days' notice and payment of applicable termination fees.	No change

				are not attended for three or more occasions, NABARD is at liberty to terminate the Contract by giving 30 days' 'Notice'. If Service Provider provides remedy within 30 days of termination notice, NABARD may reconsider its decision of termination. h. If the SLA penalties/Liquidated damages during the operations phase (Post Go-Live) calculations equals or exceed 10% of the billing for six consecutive months i. In addition to the cancellation of purchase order, NABARD reserves its right to invoke the Performance Bank Guarantee given by the Service Provider after giving notice. j. Termination in all circumstances will mean a proper transition with data transfer in a readable format along with all knowledge documents. Transition to take within a month unless extended by mutual consent. k. NABARD, without prejudice to any other remedy for breach of contract, by giving 30 days' written notice of default sent to Service Provider and if Service Provider fails to cure the default within the		

				notice period, may terminate this Contract in whole or in part.		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
402	Payment Terms and Conditions	1	1	Invoices shall be generated on monthly basis, reflecting the SLA levels for that month, and will include any applicable penalties.	Invoices shall be generated and submitted on a monthly basis, no later than the [Xth] business day of the following month, irrespective of the finalization of SLA performance data. Where SLA data is not finalized at the time of invoicing, the invoice shall be issued based on the available data. Any applicable penalties or adjustments resulting from the finalized SLA performance shall be accounted for in the subsequent month's invoice as a credit or debit, as appropriate	No change
403	QCBS Evaluation Criteria	5		Annexure I Customers for whom the Bidder has executed similar projects (To be submitted by the bidder)	Kindly consider submission of this format from bidder.	Please refer to the RFP
404	General			Additional Point	Request you to allow the credentials of Bidder's group company/ Sister concern/Affiliate for the purpose of meeting eligibility and evaluation criteria under this RFP.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
405	Minimum Eligibility Criteria	13	Annexure V	Power of Attorney (To be executed on a non-judicial stamp paper of ₹200/-)	Board resolution being a superior document than a Power of Attorney (POA). Request you to also consider submission of Board resolution for the Power of Attorney on stamp paper.	Bidder may submit either the POA or Board resolution attested by CS of the bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
406	Service Level Agreement	37	3.1.(1)	SLAs for Security Solutions viz. SIEM, SOAR, WAF, DAM, SWG, PAM, EDR, EASM, TIP, SCM, NBAD on individual basis Uptime Availability of each of the Security Tools	Request you to consider minimum uptime measured on monthly basis for each individual security tool to be 99.5% in place of mentioned 99.982 % Also request you to consider penalty impact / level as per the following. Minimum 99.982% up time measured on a monthly basis for individual security too --> NIL >= 99.8% to <99.982% up time measured on a monthly basis for individual security tool --> NIL >= 99.7% to <99.8% up time measured on a monthly basis for individual security tool --> NIL >= 99.6% to <99.7% up time measured on a monthly basis for individual security tool ---> 2 >= 99.5% to <99.6% up time measured on a monthly basis for individual security tool ---> 3 <99.50% up time measured on a monthly basis for individual	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					security tool ---> 4 Also total Penalty to not exceed 5% of Annual contract value.	
407	Service Level Agreement	38		The bidder shall ensure that there shall never be a single instance where the Security Setup is down	Request you to relax this clause / requirement considering certain unforeseen conditions / cirumstances.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				for more than 15 minutes in a single stretch.		
408	Service Level Agreement	38	3.2.(1) and (2)	SLAs for Support Operations for Security Solutions Time to Resolve – Severity 1 Time to resolve – Severity 2, 3 and 4	Request you to consider the following SLA's for resolution based on severity. a) Severity 1 ---> 4 Hours b) Severity 2 ---> 12 Hours c) Severity 3 ---> 24 Hours d) Severity 4 ---> 72 Hours Also, for penalty, Time to Resolve – Severity 1, Severity 2, 3 --> Impact Level should not go beyond 3. Also, total Penalty to not exceed 5% of Annual contract value.	No change
409	Service Level Agreement	38	3.2. (3)	SLAs for Support Operations for Security Solutions Percentage of re- opened incidents	Request you to consider target for percentage of re-opened tickets to be less than or equal to 5 % in place of mentioned 3% Also, for penalty, Percentage of re-opened incidents --> Impact Level should not go beyond 3.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					Also, total Penalty to not exceed 5% of Annual contract value.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
410	Service Level Agreement	39	3.3.(1)	SLAs for updates and upgrades Upgrades for all Components provided as part of the RfP	Based on aspects like technical feasibility, availability of downtime / change window, change management processes etc., request you to consider target to be 100% systems within 3 to 6 months from release of latest (n) version. Also consider the following penalty / impact level in place of given values. Upgrades for all Components provided as part of the RFP = 100% ---> Nil >= 99% & < 100% ---> NIL >= 98% & < 99% ---> 1 >= 97% & < 98% ---> 1.5 <97% ---> 2 Also, total Penalty to not exceed 5% of Annual contract value.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
411	Service Level Agreement	39	3.3.(2)	SLAs for updates and upgrades MIS Report	Request you to consider MIS report submission every Wednesday in place of every Monday for the previous week data i.e. from Monday to Sunday. Also, total Penalty to not exceed 5% of Annual contract value.	No change
412	Service Level Agreement	39	3.3.(3)	SLAs for updates and upgrades Patch Management for applicable systems (Security components and tools, etc.)	Request you to consider the following timelines for patch installation based on its priority considering aspects like technical dependencies, change management processes, patch testing etc. a) Critical - 7 Days b) High - 14 Days Also consider the following penalty / impact level in place of given values. 100% ---> Nil >= 99% & < 100% ---> NIL >= 98% & < 95% ---> 1 <95% ---> 2	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					Also, total Penalty to not exceed 5% of Annual contract value.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
413	Service Level Agreement	40	3.3.(4)	SLAs for updates and upgrades Vulnerability assessment and Penetration Testing Closure	Request you to consider the following timelines for closure of vulnerabilities based on its priority considering aspects like technical dependencies, change management processes, patch / configuration testing etc. a) Critical - Within 5 Working Days b) High - Within 10 Working Days c) Medium - Within 15 Working Days d) Low - Within 20 Working Days	No change
414	Service Level Agreement	41	3.5.(1)	SLAs for Service Desk Availability of helpline at service desk location	Request you to consider the following penalty / impact level in place of the given values. Upto 97% up time measured on a monthly basis ---> NIL = 92% to < 97% up time measured on a monthly basis ---> 2 < 92% up time measured on a monthly basis ---> 1	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					Also, total Penalty to not exceed 5% of Annual contract value.	
415	Service Level Agreement	41	3.5.(2)	SLAs for Service Desk Service Desk ticket/Incident Response time	Request you to consider Target time as 30 minutes in place of the mentioned 15 mins. Also, consider the following penalty / impact level in place of the given values. 100% within the defined target ---> NIL >=99% and <100% meeting the target ---> 1 >=97% and <99% meeting the target ---> 2 >=95% and <97% meeting the target ---> 3 Finally, total Penalty to not	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					exceed 5% of Annual contract value.	
416	Service Level Agreement	42	3.6	SLAs for Incidence Response Incidence Response	Request you to consider the following penalty / impact level in place of the given values. <=30 mins ---> Nil >30 mins and <=60 mins ---> 3 >60 mins and <=90 mins ---> 2 >90 mins and <=180 mins ---> 1 Finally, total Penalty to not exceed 5% of Annual contract value.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
417	Minimum Eligibility Criteria	2	7	Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024-25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches (This shall override experience criteria given in the bid in other documents)	Request to kindly amend the clause as below: Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed **Any** SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed (PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 **2** distinct clients in the last 5 years (FY 2024- 25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at least one (1) PO should be of a Schedule Commercial Bank **(Govt/Large Private Company/Public listed Company)** in India having more than 1000 branches. (This shall override experience criteria given in the bid)	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
418	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/GCFE/ CHFI/ ECSA/CREST/ CISM/ CISA/OSCP/ CEH certified. Note: (i) Resources for CEH Max 10 resources shall be onsidered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource is carrying more	Request to kindly amend the clause as below: The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 **10** professionals should be CISSP/ GCFA/ GCIH/GCFE/ CHFI/ ECSA/CREST/ CISM/ CISA/ OSCP/ CEH certified. Note: (i) Resources for CEH Max 10 resources shall be onsidered. The certification date must be	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				than one certification, it shall be considered as one.	prior to the date of publication of this RFP. (ii) If a resource is carrying more than one certification, it shall be considered as one.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
419	Minimum Eligibility Criteria	1	2	Financials a. Minimum Average Annual turnover criteria for the past 3 financial years (2023-24, 202223 and 2021-22) for the bidder should be 120 Crore. b. The bidder should have positive operating profit during the last three financial years (2023-24, 2022-23 and 2021-22). c. Further, Net worth of the Bidder should be positive as on the end of the 31 March 2024. Supporting Document, Copy of, A. Audited profit and loss statements and balance sheet of the three financial years (2023-24, 2022-23 and 2021-22) and B.**Certificate form statutory auditor/CA as per Annexure I**	We have CA Certiifcate Letter with all the details mentioned as per Anenxure I. Request NABARD to kindly consider that Letter against Anenxure I	No Change
420	Minimum Eligibility Criteria	4	12	Power of attorney: Power of attorney to be executed as per annexure V.	We have a standard Power of Attorney (POA) document, duly notarized and signed by the authorized signatory on a ₹500/- stamp paper. We kindly request the customer to accept this format, as it is the standard	Bidder may submit the standard PoA as part of the bid submission

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					document submitted for all RFPs. Request NABARD to kindly consider the same against Annexure V.	
421	QCBS Evaluation Criteria	2	B.(1)	Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22, 2020-21 (Bidder shall submit PO/credential letters) a)03 to 05 projects - 3 Marks b)06 to 07 projects - 4 Marks c)08 projects and above - 5 Marks	Request to kindly amend the clause as below: Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22, 2020-21 (Bidder shall submit PO/credential letters) a)**01** 03 to **03** 05 projects - 3 Marks b)**04** 06 to **06** 07 projects - 4 Marks c)**07** 08 projects and above - 5 Marks	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
422	QCBS Evaluation Criteria	2	B.(1)	Additionally, if the submitted POs as per the above criteria pertain to the BFSI clients, additional marks as below shall be allocated a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks	Request to kindly amend the clause as below: Additionally, if the submitted POs as per the above criteria pertain to the BFSI/**Large Private Organization/Public Listed Comapany** clients, additional marks as below shall be allocated a)**01** 03 to **03** 05 projects - 3 Marks b)**04** 06 to **06** 07 projects - 4 Marks c)**07** 08 projects and above - 5 Marks	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
423	Scope of Work and Technical Specifications	3	(j)	Procurement, Supply, Installation, Commissioning, operation, administration & maintenance of all the components & sub-components including all necessary hardware & related software (including licenses) as per the proposed solution will be the Bidder's responsibility.	Will any hardware which is required for the IT components be provided by NABARD through their DC or the same has to be brought by the bidder? If yes, are there are specifications for the hardware which is to be procured?	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.
424	Scope of Work and Technical Specifications	4	(y)	Licenses for the entire project may be procured in the name of the vendor or NABARD. However, any such arrangements should not violate the licensing policy of any OEM. The service provider shall be liable for any punitive action or damage for violation of licensing policies.	Bidder suggests that NABARD may go for pure MSSP services wherein all the responsibility of procurement / management/provision of services will lie with the bidder. If licenses are to be procured in the name of NABARD, then this should be a SI driven and OEM led RFP which will be on CAPEX basis. But since NABARD is	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					looking for "as a service" model, bidders suggests going for subscription model RFP.	
425	Scope of Work and Technical Specifications	1	1.(b)	The solution will be procured on an operational expenditure (Opex) basis, ensuring high availability and allowing for a rate contract to accommodate any additional or enhanced requirements as they arise.	Bidder suggests that NABARD may go for pure MSSP services wherein all the responsibility of procurement/management/provision of services will lie with the bidder. If licenses are to be procured in the name of NABARD, then this should be a SI driven and OEM led RFP which will be on CAPEX basis. But since NABARD is looking for "as a service" model, bidders suggests going for subscription model RFP.	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
426	Scope of Work and Technical Specifications	1	1.(a)	The RFP seeks to engage a Managed Security Service Provider (MSSP) for providing managed SOC services across the proposed Bank's Infrastructure which consists of Private Cloud spanning across DC, DR and near Site. This includes the procurement of necessary hardware and related tools, as well as the ongoing operations and management of the entire Security solution. The entire solution has to be maintained over a five-year period from the go live date. NABARD may further extend the contract beyond a term of 5 years on a mutual agreement basis	Bidder suggests that the SOC operations and management should be delivered entirely remotely as most MSSPs deliver SOC services through their offsite SOC/ ODC centers.	Kindly refer to corrigendum
427	Scope of Work and Technical Specifications	1	2.(d)	Integration of components (hardware/software) with each other and the Bank's Infrastructure and with third party devices is the sole responsibility of the selected bidder. Besides, the bidder has to ensure that their tools are integrated in the Bank's / its Cloud provider portals viz., SLA portal, Invoice portal, Service Desk portal, Bird's eye view Dashboard etc.	MSSP has own set of portals and dashboards available plus management tools zone. Dedicated portal for SLA reporting with role based access can be provided to NABARD officials	In addition to the dashboard provided by the bidder the same shall be integrated with the Bank's Online portal.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
428	Scope of Work and Technical Specifications	2	(f)	Bidder shall make necessary measures for security of the infrastructure for threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, ransomware, botnets etc. and shall provide protection against network issues such as traffic and routing instability.	Bidder suggests removal of DDOS scope from MSSP scope of work and ransomware and botnets management can be availed from respective CSP/MSP	Bidder shall configure all the security solutions to prevent DDOS and DOS attacks.

429	Scope of Work and Technical Specifications	17	9	Responsibility Matrix	1. What part of data/network/application security is to be owned by the MSSP? Security of the cloud is responsibility of the respective CSP/MSP 2. Regulatory compliances cannot be owned by MSSP and need to be managed by NABARD/respective third party service providers 3. VAPT recommendations cannot be owned by MSSP as MSSP is not responsible for performing VAPT 4. Is VAPT before go-live to be performed by MSSP? If yes, the same should be included in the commercial bid. 5. Security Policy updates need to be managed by NABARD. If NABARD expects formulation of security policy by bidder, the same needs to be included in commercial bid 6. DLP and DDOS have not been included in commercial bid.	1. Kindly refer to the RFP 2. MSSP shall be configure all security solutions as per regulatory compliances. 3. Closure of VAPT observations pertaining to security solutions is the MSSP bidder's responsibility. 4. VAPT is to be performed by VAPT service provider. However, the recommendations of VAPT should be closed as per the timelines specified in the RfP 5. Bidder has to prepare the security policies in consultation with the Bank. 6. DLP and DDOS are not part of the solutions to be provided by the MSSP

					7. Is security awareness training part of MSSP scope? If yes, how many officers need to be trained? What will be the frequency and duration of these trainings? What will be the content that needs to be covered in these trainings? Request NABARD to include these trainings in the commercial bid.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
430	Scope of Work and Technical Specifications	1	2.(a)	The bidder must deliver managed security services for NABARD, ensuring that the entire solution is deployed at NABARD designated locations on pay-as-you-go model. This approach aims to ensure that NABARD's infrastructure is both secure and scalable, meeting the organization's evolving needs over the contract period.	Many of the services which have been asked for in the RFP are SaaS-based services for which the deployment as NABARD designated location is not feasible. As detailed in query number 2, bidder suggests that NABARD should go for MSSP model wherein all the services would be taken care of by the bidder.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
431	Scope of Work and Technical Specifications	1	2.(b)	The solution shall include Supply, Installation, Implementation, Integration, Roll Out, Operations and Maintenance of all the security tools listed in this RFP in DC, DR and Near site for the entire contract duration: Security Information and Event Management (SIEM) as a service Security Orchestration Automated Response (SOAR) as a Service Incident analysis, response and management services Threat hunting Service Web Application Firewall (WAF) as a service Secure Web Gateway (SWG) as a Service Database Activity Monitoring (DAM) as a Service Privilege Access Management (PAM) as a Service External Attack Surface Management as a Service Endpoint protection with EDR as a service Network Behavior Anomaly Detection (NBAD) as a service.	There are many tools which have been defined in the RACI matrix which are falling under MSSP prerogative but have not been included in the commercial bid. Request NABARD to add the same in the commercial bid.	Please refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				Threat Intelligence Platform as a service Security Compliance Management (SCM) as a service		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
432	Scope of Work and Technical Specifications	2	2.(h)	The bidder will be responsible for providing deployment and 24X7X365 operational support for all the security tools proposed in this RFP, which includes, but is not limited to: Design and Architecture: Crafting the overall structure and design of the cloud infrastructure.	This clause seems to have seeped through in the RFP from a previous cloud RFP. The bid circulated deals with MSSP services and the design of cloud infrastructure is off limits of bid scope. Kindly look into the same.	Kindly refer to corrigendum
433	Scope of Work and Technical Specifications	3	2.(v)	All the components procured by the bidder as part of the solution shall have 5 years of Warranty/ AMC from the go-live date. Besides, the components procured by the bidder shall not reach EOL/EOS/EOSL during the contract period.	EOL/EOS/EOSL come in the picture when we talk about CapEx model. NABARD, as can be seen from the deal scope of work, seems keen on an MSSP model wherein all licenses, tools, solutions will be managed by the bidder. As per point 2 of the queries, request NABARD to go for MSSP model wherein all services will be managed by bidder in "as a service" model and NABARD shall not have to worry about licenses and EOL of components, etc.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
434	Scope of Work and Technical Specifications	4	2.(bb)	Bank will periodically review the process of handling of the alerts / events related to SOC services. All SOC policies, procedures and playbook to be drafted by the bidder and reviewed and approved by the bank. All the policies and procedures shall be reviewed on an annual basis/or as per the Bank's requirement.	Request NABARD to clarify if the security policies have to be drafted by the bidder. If yes, request NABARD to include the same in the commercial bid.	Bidder has to draft the security policies as per the industry practice after approval from NABARD.
435	Scope of Work and Technical Specifications	4	2.(ff)	Bidder has to ensure proper archival, purging and retention of logs for future analysis as per the Bank's requirement. Further, the bidder has to provide independent assurance for purging of logs after termination/ end of contract.	Request NABARD to clarify as to who would be providing the storage for the logs.	NABARD will be providing storage for the logs
436	Scope of Work and Technical Specifications	3	2.(m)	The entire solution shall be scalable at short notice within 1 month of the request from NABARD and shall be governed by SLA.	It would be necessary for the bidder to have visibility on the current log volume and the asset inventory to ensure that the solution offered by the bidder comes with assurance of scalability. Also, OEMs have lead time of 12 to 16 weeks for any product which will make delivery difficult in procurement model.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					Through MSSP model, the same can be delivered in requested timeframe or even immediately.	
437	Scope of Work and Technical Specifications	2	2.(i)	Bidder shall support business continuity plans as decided by NABARD or any other entity approved by NABARD from time to time.	This may lead to additional scope which may not be accounted by the bidder beforehand. Request NABARD to specify what is meant by "any other entity".	The same shall be shared with the successful bidder.
438	Scope of Work and Technical Specifications	5	2.(mm)	All the tools proposed as part of the RFP shall be integrated with the existing infrastructure of the Bank, ensuring seamless integration of all the solutions among themselves.	Please share the versions, makes/models, count and log formats of infrastructure components to be integrated (e.g., firewalls, DBs, routers, endpoints, WAF, PAM, DAM). This will ensure parser/connector readiness from the MSSP side. This will also be required for planning the time which would be required for the integration process and to ensure compatibility with the	The same shall be shared with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					offered tools and solutions. Request NABARD to share the inventory of the same.	
439	Scope of Work and Technical Specifications	5	3.1.1	The SIEM solution shall seamlessly integrate with Bank's existing infrastructure devices like servers, switches, routers, SDWAN, DB, Applications, AD, Email gateway, firewall devices, backup devices etc and proposed security solutions of the RFP such as SOAR, PAM, DAM, WAF, AV, EDR, etc.	Please share the versions, makes/models, count and log formats of infrastructure components to be integrated (e.g., firewalls, DBs, routers, endpoints, WAF, PAM, DAM). This will ensure parser/connector readiness from the MSSP side. This will also be required for planning the time which would be required for the integration process and to ensure compatibility with the offered tools and solutions. Request NABARD to share the inventory of the same.	The same shall be shared with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
440	Scope of Work and Technical Specifications	5	3.1.2	The SIEM solution must be capable of storing 6 months live logs. After the period of 6 months the logs should be archived for the entire contract period. The logs collection should be done at NABARD's site or its appointed agencies' site	Please confirm whether archived logs must be readily searchable or only retrievable on request. Also clarify if raw logs or indexed/processed logs are expected for long-term storage.	The logs should be readiy searchable in order to retrieve on request
441	Scope of Work and Technical Specifications	5	3.1.3	The offered SIEM solution should support 10000 EPS (Events per Second) and/or equivalent Flow records per second with 30% buffer capacity at initial level. The proposed solution must have the functionality to scale both horizontally and vertically and scalability.	1. Please clarify if 10,000 EPS is cumulative across all locations or per site (DC, DR, Near Site). This will help the bidder propose the appropriate SIEM solution for NABARD. 2. Also confirm whether HA is expected to be active-active across sites for both collection and correlation components. Also request NABARD to clarify if this 10000 eps is for day1 of go-live or for entire contract duration. When will billing start for these logs? 3. Please confirm if the 10,000 EPS includes both event and	1. 10000 EPS is cumulative for all three locations. Bidder also needs to keep buffer as proposed in the RFP. 2. HA is expected at all three sites in Active active mode. 3.Kindly refer to the RFP.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					flow logs or is exclusive to events. What is the baseline for EPS calculation (compressed/uncompressed, raw/parsed)?	
442	Scope of Work and Technical Specifications	6	3.1.8	The bidder to share the above-mentioned reports with Bank: a. Use cases implemented (Weekly) b. Use cases triggered (Realtime) c. Log sources not triggering (Realtime) d. Utilization report in EPS (Weekly) e. Incident report (Daily, Weekly and Monthly) f. SIEM Inventory (Weekly)	1. Please confirm if MSSP can use its own secure dashboard/reporting portal for scheduled SIEM reports or if Bank will provide its own portal for integration and uploads. 2. Please specify required formats (Excel, PDF, CSV, etc.) and delivery method (email, portal, API) for SIEM reports such as EPS utilization, log	1. In addition to the dashboard provided by the bidder the same shall be integrated with the bank's Online portal. 2. The same shall be discussed with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					source status, and use case triggers.	
443	Scope of Work and Technical Specifications	5	3.1.6	The proposed SIEM tool should be an advanced AI/ML-based solution. It must leverage artificial intelligence and machine learning technologies to enhance its predictive capabilities. This will enable the system to proactively identify potential security threats and vulnerabilities before they can be exploited. The tool should be capable of analyzing vast amounts of data in real-time, detecting anomalies, and providing actionable insights to mitigate risks. Additionally, itshould offer automated response mechanisms to swiftly address any identified threats, ensuring robust security	Is NABARD expecting a natively AI/ML-enabled SIEM platform, or can MSSP propose a third-party ML analytics engine? Should pre-trained models be demonstrated during bid evaluation?	Kindy refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				posture and compliance with industry standards.		
444	Scope of Work and Technical Specifications	5	3.1.4	Installation and commissioning of adequate log collector at Bank sites (DC, DR and Near Site). Ensure that logs are being collected from all the in-scope devices. As appropriate suggest Bank and related stakeholders on required log-levels and support Bank in enabling the suggested log levels.	Please confirm whether MSSP should enable all suggested log levels or if the final decision depends on performance impact and criticality as advised by MSSP experts.	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
445	Scope of Work and Technical Specifications	5	3.1.5	The bidder must provide the bank with read/write access to the SIEM platform.	Please clarify what actions NABARD is expected to perform with write access—such as rule creation, dashboard design, or alert handling—and whether any role-based access restrictions apply.	The same shall be shared with the successful bidder.
446	Scope of Work and Technical Specifications	6	3.2.2	The proposed SOAR solution should be seamlessly integrated with the proposed SIEM solution and Bank's infrastructure along with the existing and proposed security devices/solution like but not limited to WAF, IPS, various firewalls, PAM, AV, EDR, PIM, PAM etc. for collecting data about security threats from multiple sources, without any extra cost to the Bank.	Please provide a list of existing security tools/devices including make/model/version and confirm if these provide API access for integration with SOAR.	The same shall be shared with the successful bidder. However, all the tools have API integration facility.
447	Scope of Work and Technical Specifications	6	3.2.3	In case there is a requirement of the integration of SOAR solution with any existing or new security device/solution within the contract period, the same is to be done by the bidder without any cost to the Bank.	Please clarify the expected frequency of such integrations and confirm if Bank will provide timely API documentation and test environments for new tools introduced during the contract.	MSSP bidder shall integrate all infra/security/network/etc devices with security solutions as and when required during entire project duration.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
448	Scope of Work and Technical Specifications	6	3.2.4	The SOAR solution should leverage advanced AI and ML techniques to enhance security operations. This includes the ability to integrate seamlessly with various security devices and solutions, automate security workflows and dynamically manage incidents. The solution should utilize machine learning for tasks such as analyst assignments, incident severity calculation and real-time threat information aggregation. Additionally, it should provide a virtual War Room for comprehensive incident investigation and collaboration and employ advanced techniques to score alerts based on criticality in real-time.	Does NABARD expect out-of-the-box AI/ML features or can these be built using third-party analytics tools integrated into the SOAR? Is there a minimum benchmark for automation accuracy?	Kindly refer to the RFP
449	Scope of Work and Technical Specifications	6	3.2.7	The Solution (with each of its components) should be configured in High Availability (HA) mode.	Please confirm whether active-active HA is expected across DC, DR and Near Site, or if an active-passive setup will suffice. What is the expected RTO/RPO for SOAR?	Bidder shall propose all the security solutions in HA under active active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
450	Scope of Work and Technical Specifications	7	3.2.10	The orchestration and automation of security workflows, eliminating manual intervention to reduce mundane tasks.	Please clarify whether the MSSP is expected to create automation playbooks from scratch or if NABARD will provide samples/templates for tailoring. Also confirm how many playbooks are expected to be operationalized initially.	The MSSP is expected to create playbooks and perform steps as mentioned from scratch for NABARD
451	Scope of Work and Technical Specifications	7	3.2.11	Leverage the automated playbooks as per the technical specification and create customized automated playbooks tailored for Bank's processes.	Will the Bank provide a baseline set of processes/playbooks or should the MSSP create all playbooks from scratch through stakeholder discussions?	The MSSP is expected to create process/ playbooks in consultation with the Bank
452	Scope of Work and Technical Specifications	7	3.2.15	SOAR solution should bring down the MTTR / manual efforts and shorten the time to resolve and investigate incidents. SOAR should integrate with all SOC and IT asset management components to ensure automation, governance, workflow etc. across all the SOC solutions and IT Infrastructure.	Please confirm what IT asset management (ITAM) tools are in use and if integration interfaces are available.	All the tools have API based integration facility
453	Scope of Work and Technical Specifications	7	3.2.16	The platform should be capable of providing detailed post incident documentation about the actions taken, root cause, controls implemented and lesson learned etc.	Please confirm if there's a preferred format or portal for incident post-mortems. Is there an expected timeline within which these documents should be provided by the bidder?	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
454	Scope of Work and Technical Specifications	7	3.2.17	Bidder shall share the below mentioned reports to Bank a. Playbook Inventory (Weekly) b. Incident report (Weekly, Monthly)	Please confirm the expected format (Excel, PDF, API-based report) and delivery mode (portal/email) for these reports. Should these reports be integrated into NABARD's dashboard or managed via MSSP's interface?	Same shall be shared with the successful bidder. These reports are also expected to be integrated with the Banks portal in additional to the sharing the reports from MSSP's interface.
455	Scope of Work and Technical Specifications	6	3.2.9	The Bidder shall provide the technical design document including a. Product details & Administrative Guide b. Troubleshooting Guide Basic and Advanced with Support andmaintenance plan. c. User guides and troubleshooting manuals. d. Solution design and architecture documentation (diagram). e. Test and validation reports.	Please clarify whether OEM-provided templates for admin guides, user manuals, and troubleshooting are acceptable, or if customized documents in a NABARD-specified format are required.	Bidder has to finalise the document format in consultation with NABARD.
456	Scope of Work and Technical Specifications	7	3.3.1	The MSSP shall perform analysis of auto-triggering alerts from a number of security products including AV, EDR, PAM, WAF, DAM, HIPS, Attack surface management, SIEM, NBAD, Web Proxy etc.	Please share the list of OEMs and tool versions in use for each of the listed technologies. Are parser/connectors for all tools already available or expected to be developed by MSSP?	Bidder shall provide the security solutions and write parsers accordingly.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
457	Scope of Work and Technical Specifications	7	3.3.2	Solution should have advanced techniques such as machine learning that considers contextual parameters, historical behavior & external threat intelligence to score an alert based on criticality in real time.	Will NABARD provide existing threat intelligence feeds (e.g., CERT-IN, FS-ISAC, commercial feeds), or should MSSP provision them? Is NABARD expecting proprietary ML algorithms or can bidder leverage SIEM/SOAR-native scoring?	Bidder shall provision all intelligence feeds from their relevant sources.
458	Scope of Work and Technical Specifications	7	3.3.3	MSSP Bidder shall develop documentation regarding IR policy, Processes, SOPs etc.	Please confirm if NABARD has an existing IR framework/policy that needs to be enhanced, or if MSSP should create all documents from scratch. What is the approval process and review frequency for these documents?	Bidder has to prepare all the mentioned documentation in consultation with NABARD.
459	Scope of Work and Technical Specifications	7	3.3.4	Bidder shall coordinate with other departments /teams /vendors for mitigation and closure of the incident.	Please confirm if NABARD will nominate SPOCs from internal teams/vendors for effective coordination and closure. Also, will a collaboration tool or platform be provided by NABARD for managing such communications?	Bank will share the SPOC details with successful bidder

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
460	Scope of Work and Technical Specifications	7	3.3.5	MSSP should provide automated incident analysis features/service for analysis of alerts received to answer the following: a. Impact on the assets b. Attributes of an attacker c. Determine other assets which may have been compromised d. Determine how long the attack campaign was & where was first compromise e. Maintain artifacts & IOCs of an incident	Does NABARD expect the MSSP to use an in-built threat analysis platform (e.g., sandbox, TI engine), or integrate with external forensic tools? Please confirm if any tools are already in use.	Bidder is expected to utilize proposed security tools i.e EDR, threat hunting, incident analysis, etc and prepare and share the details report with all the mentioned details i.e. point 'a' to 'e'.
461	Scope of Work and Technical Specifications	8	3.3.6	MSSP to describe how it performs a strong Incident Response Mechanism in providing Bank with comprehensive information about a potential incident, assemble the appropriate context, investigate as to make recommendations so that Bank starts containment & remediation activities.	Will NABARD provide a sample incident severity matrix or prioritization logic that MSSP must follow or can MSSP propose its own based on industry best practices?	MSSP can propose the best practices followed in the industry subject to approval of NABARD

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
462	Scope of Work and Technical Specifications	8	3.3.7	Bidder should maintain an Incident Management Plan with at least the following: a. Incident Management Plan & Governance b. Incident Response plan & Governance c. Workflows for Incident Management & Response d. Communications & escalations Plan, Process & Metrics	Please confirm if templates or frameworks (e.g., NIST, ISO 27035) should be followed for documentation. Also, how often should these plans be reviewed and updated (e.g., quarterly/annually)?	Bidder shall finalize the document in consultation with the Bank.
463	Scope of Work and Technical Specifications	8	3.3.8	The scope shall include the Bank's DC, DR, Near Site and other security tools proposed by MSSP bidder.	Please confirm whether on-site presence is required at all three locations or remote 24x7 delivery is acceptable, with on-demand site visits.	No onsite presence is required. However Bank may request for on-demand site visit at no additional cost.
464	Scope of Work and Technical Specifications	8	3.3.9	The bidder has to provide incident response and management services on 24*7*365 basis.	Please clarify expected average monthly incident volume and SLA for response and resolution times (e.g., T1, T2, T3).	Kindly refer to SLA
465	Scope of Work and Technical Specifications	8	3.3.10	The bidder shall be responsible for Reporting and logging of information security incidents through the use of Bank's ticketing tool.	Please confirm the make and API capability of the ticketing tool. Will integration for auto-ticket creation via SIEM/SOAR be allowed?	Same shall be shared with the successful bidder

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
466	Scope of Work and Technical Specifications	8	3.3.10	Bidder shall share weekly and quarterly reports of incidents along with: a. No. of incidents triggered. b. No. tickets with SLA breached. c. Open tickets d. Closed tickets e. Category-wise tickets.	Please confirm if reports need to be shared only in PDF/Excel or if there is a requirement to auto-upload into a Bank-owned dashboard/portal. Also, is any specific visualization/dashboarding tool preferred?	The reports are also expected to be integrated with the Banks portal in additional to the sharing the reports from the MSSP's interface.
467	Scope of Work and Technical Specifications	8	3.4.1	The bidder must facilitate threat hunting using hypothesis driven, IOC-driven, analytics-driven methods and situational along with emerging threats.	Please clarify whether NABARD expects daily/weekly/monthly frequency of each type of hunting (IOC-driven, hypothesis-driven, etc.). Can MSSP decide frequency based on evolving threat landscape?	Threat hunting service is required on daily basis. Further, frequency can be changed in case of increased threats.
468	Scope of Work and Technical Specifications	8	3.4.2	The hunting framework should be defined, developed, implemented, updated and maintained to encompass the creation of objective-based strategic hunt missions aimed at identifying unalerted malicious activity, along with the search for IOC provided by Threat Intelligence and Analytics.	Does NABARD have a baseline framework (e.g., MITRE D3FEND or ATT&CK) or is the MSSP expected to propose the entire framework? Will this framework require formal review/approval by the Bank?	The bidder shall create and provide threat hunting framework in consultation with the Bank.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
469	Scope of Work and Technical Specifications	8	3.4.3	The bidder should be flexible to allow customization and adaptation of the threat hunting process according to the Bank's unique needs and specifications.	Please confirm if customization needs to be done tool-wise (TIP, SIEM, EDR) or only at the process/playbook level. Will NABARD provide onboarding sessions to understand internal threat modeling practices?	Bidder may propose the best available method. The bidder shall create and provide threat hunting SOP in consultation with the Bank.
470	Scope of Work and Technical Specifications	8	3.4.4	The bidder should provide the capability for both manual and automated threat hunting.	Please confirm if NABARD will provide any existing tools or licenses for manual hunting (e.g., ELK stack, Kibana, Splunk dashboards) or if all tooling must be proposed by MSSP.	All the tools must be proposed by Bidder.
471	Scope of Work and Technical Specifications	9	3.4.7	The bidder is required to possess a Threat Intelligence Platform (TIP) to supply Indicators of Compromise (IOC) to the Bank, in addition to the Threat Intelligence feed received by the SIEM	Is there a preference or whitelist of approved Threat Intelligence Platforms (TIPs)? Should TIP be hosted on NABARD infra or MSSP infra (with sovereignty compliance)?	Bidder may propose the best available method and solution
472	Scope of Work and Technical Specifications	9	3.4.8	The vendor should provide detailed custom reports on newly discovered malicious threats and malware.	Please specify the expected format and depth of malware reports. Should sandboxing/detonation reports also be included, and will Bank provide access to such tooling or expect MSSP to provision?	The format of the report shall be mutually agreed upon by NABARD and the bidder. The bidder shall prepare the report for NABARD accordingly

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
473	Scope of Work and Technical Specifications	9	3.4.10	The bidder should share periodic (weekly) threat advisories as per Bank's requirements and depending on the threat environments as per Bank's threat landscape.	Will NABARD define the advisory structure (e.g., TLP classification, sector-specific advisories), or can MSSP use their standard threat bulletin format?	Formats shall be finalised on mutual discussion between the successful bidder and NABARD.
474	Scope of Work and Technical Specifications	9	3.4.11	The bidder must provide visual representations like charts for (but not limited to) prominent attacks and attackers, threat analysis based on OWASP and MITRE ATT&CK, emerging threat trends, attack demographics, etc. in consideration with all the in-scope assets of Bank. These reports should provide comprehensive information, focusing on attack vectors, channels, and methods.	Please confirm the preferred format (PDF, PowerBI, web dashboard) and frequency of such visual reports. Is NABARD expecting drill-down interactivity or static reporting?	Formats shall be finalised on mutual discussion between the successful bidder and NABARD.
475	Scope of Work and Technical Specifications	9	3.4.13	The bidder must ensure to have automated playbooks for threat hunting. The vendor should deliver proactive threat hunting services across networks, endpoints, and unusual user behavior. This aids in identifying advanced attacks such as (but not limited to) lateral movement, malware beaconing,	Can these playbooks be MSSP-owned or must they be co-created and approved by NABARD? Also, how many initial playbooks are expected to be created during onboarding?	All the playbooks must be approved by NABARD

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				data exfiltration, watering hole attacks, process anomalies, service anomalies, and account takeovers.		
476	Scope of Work and Technical Specifications	9	3.4.15	The bidder should formulate hypotheses about potential threats based on knowledge of current threat landscapes, vulnerabilities, and industry-specific risks.	Will NABARD provide a list of known assets, vulnerabilities (via VA/PT or tools like Qualys/Tenable), and industry-specific threat scenarios for shaping these hypotheses?	Bidder has to provide its own set of threat scenarios relevant to the industry
477	Scope of Work and Technical Specifications	9	3.4.18	The bidder should ensure that malware scanning, protection, presentation, and reporting are implemented according to the Bank's specific requirements.	Will NABARD share specific malware policies or tool preferences (e.g., sandbox, signature-based AV, behavioral detection)? Also, are any malware tool licenses already available with the Bank?	Bidder has to provide all the tools and licenses as requested in this RFP.
478	Scope of Work and Technical Specifications	9	3.4.19	The bidder should provide recommendations for mitigating threats and vulnerabilities based on findings, often working closely with incident response teams.	Is the recommendation expected as part of standard monthly reports or in real-time following detection? Should these also be uploaded to a ticketing system?	Bidder is expected to followup in Real time for any issues. All these should be uploaded to the ticketing system.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
479	Scope of Work and Technical Specifications	10	3.4.20	The bidder should thoroughly document all findings, actions taken, and lessons learned during the threat hunting process to improve future efforts and maintain a historical record and provide a monthly report	Please confirm the expected review process and format for lessons learned documentation. Should it be included in the same report as threat findings, or as a standalone submission?	Same shall be shared with successful bidder.
480	Scope of Work and Technical Specifications	10	3.4.21	The bidder should continuously refine and adapt threat hunting techniques and processes based on lessons learned and emerging threats.	Will NABARD require quarterly performance reviews of the threat hunting effectiveness with metrics such as dwell time reduction, false positive rate, etc.?	Please refer to the RFP.
481	Scope of Work and Technical Specifications	12	3.8.1	The bidder shall be responsible for supply, implementation, maintenance and support of Attack Surface Monitoring Solution for assets accessible publicly.	Please confirm whether NABARD has an existing EASM solution or expects the bidder to propose a new OEM. Also clarify whether on-prem deployment is allowed or SaaS-only model is preferred.	Bidder has to provide a new EASM solution
482	Scope of Work and Technical Specifications	12	3. 8.2	The EASM solution shall be seamlessly integrated with Bank's existing infrastructure devices and the proposed solution such as AD, SIEM, Firewalls, etc. The integration shall be carried out by the bidder.	Please confirm if these integrations will be API-based. Are these systems on-premise, hybrid, or cloud-hosted? Will test credentials and sandbox environment be provided?	Please refer to the RfP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
483	Scope of Work and Technical Specifications	12	3.8.3	The proposed EASM solution should discover and map all external assets.	Please confirm if NABARD will provide a list of known domains / Ips / subdomains to initiate discovery or whether the MSSP is expected to begin with OSINT-based enumeration.	Bidder may propose the best available method
484	Scope of Work and Technical Specifications	12	3.8.4	The bidder is expected to manage EASM solution 24*7*365 and follow SLA.	Please confirm the SLA expectations for incident triage from real-time alerts and if automated mitigation is required.	Automated mitigation is envisaged
485	Scope of Work and Technical Specifications	12	3. 8.6	The proposed EASM solution should identify and prioritize vulnerabilities for remediation.	Please confirm if the bidder can use proprietary CVSS-based scoring or if NABARD has its own threat/vulnerability rating matrix to be followed.	Bidder may propose the best available method
486	Scope of Work and Technical Specifications	12	3.8.8	The bidder shall share the following mentioned reports as per defined frequency a. External assets report (Daily) b. Incident summary (Daily)	Please confirm preferred format (Excel, PDF, Dashboard) and if reports need to be pushed into NABARD's SOC portal automatically via API or manually uploaded.	In addition to the dashboard provided by the bidder the same shall be integrated with the bank's portal.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
487	Scope of Work and Technical Specifications	12	3.9.1	The bidder shall be responsible for supply, implementation, maintenance and support of EPP and EDR by providing integrated detection, analysis, and response across the organization's endpoints/servers present in the Bank's Data Centre, Disaster Recovery Centre and Near Site.	Please share estimated endpoint/server count to be covered. Are virtual/remote endpoints also part of the scope (e.g., staff on VPN)?	Please refer to the BOM
488	Scope of Work and Technical Specifications	12	3.9.2	The EPP with EDR solution shall be seamlessly integrated with Bank's existing infrastructure devices and proposed solutions such as AD, SIEM, Firewalls etc. The integration shall be carried out by the bidder.	Please confirm whether existing EDR agent (if any) will be replaced or co-exist. Is MSSP expected to handle uninstall/redeploy tasks across all endpoints?	Bidder has to provide a new EDR solution with EPP from scracth.
489	Scope of Work and Technical Specifications	12	3.9.3	The proposed EPP and EDR solution should Identify advanced and unknown threats through integrated visibility.	Please confirm if the Bank expects an OEM with native behavioral/heuristic engines, or MSSP-developed custom rules can be used in existing tools.	Please refer to the RfP
490	Scope of Work and Technical Specifications	12	3.9.4	The proposed EPP and EDR solution should Configure detection rules, policies, and automated workflows	Can the MSSP define baseline rules, or should they strictly align to policies provided by NABARD? Will there be a rule approval board?	MSSP will compile the rules in consultation with NABARD

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
491	Scope of Work and Technical Specifications	12	3.9.5	The proposed EPP and EDR solution should reduce response time with automation and orchestration capabilities.	Please confirm if the MSSP can integrate EDR response with SOAR platform proposed under the SOC. Is this expected from day one or as part of a phased approach?	All the solutions/services mentioned in the RFP along with the integration is expected from Day 1 of the project
492	Scope of Work and Technical Specifications	12	3.9.6	The EDR solution should meet all the technical/functional specifications of the solution as specified in the Technical Specification sheets.	Kindly confirm if NABARD has preferences for specific OEMs or product families. Also confirm whether MSSP has the flexibility to propose multi-OEM deployment (e.g., one for endpoints, one for servers).	Bidder may propose the best available solution
493	Scope of Work and Technical Specifications	12	3.9.7	The bidder shall share following reports in the defined frequency a. Incident report (Daily) b. Action taken report (Daily) c. Quarantine report (Daily) d. Coverage report (Daily)	Will NABARD provide a reporting template or is bidder expected to define this? Will integration into Bank's dashboard be required for real-time visualization?	The reporting template may be finalised by NABARD in consultation with the successful bidder. Integration into Bank's dashboard is also required.
494	Scope of Work and Technical Specifications	14	3.12.1	The bidder shall be responsible for supply, implementation, maintenance and support of TIP solution across the organization's endpoints /servers present in the Bank's infrastructure.	Please confirm if NABARD has any existing TIP or threat intelligence arrangement (e.g., from CERT-IN, FS-ISAC, OEM-based feeds) to be integrated, or MSSP must provision a fresh TIP with licensed feeds.	MSSP has to provide the fresh TIP services.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
495	Scope of Work and Technical Specifications	14	3.12.2	The TIP solution shall be seamlessly integrated with the Bank's existing infrastructure devices and the proposed solutions such as AD, SIEM, Firewalls, etc. The integration shall be carried out by the bidder	Kindly share the list of integration targets (tools and OEMs) to validate TIP compatibility and connectors. Will NABARD provide sandbox/test access to validate integration readiness?	In addition to the tools provided by the bidder, it has to be integrated with the Cloud infrastructure and tools.
496	Scope of Work and Technical Specifications	14	3.12.3	The solution should be able to Collect threat data from various sources, including internal logs, external threat feeds, and open-source intelligence.	Is the MSSP allowed to use third-party commercial threat feeds (e.g., Recorded Future, Mandiant, Anomali) or is NABARD expecting use of only open-source and community feeds?	Bidder may propose the best available method and solution
497	Scope of Work and Technical Specifications	14	3.12.5	Analyzes the aggregated data to identify patterns, correlations, and potential threats. This helps in understanding the tactics, techniques and procedures (TTPs) of threat actors.	Does NABARD expect TTP mapping to follow MITRE ATT&CK framework? If yes, can MSSP use proprietary mapping models or Bank-prescribed standards?	Bidder may propose the best method available for the same
498	Scope of Work and Technical Specifications	14	3.12.6	The solution shall continuously update and refine threat intelligence to keep up with the evolving threat landscape.	Please clarify if there is a preferred refresh rate/frequency expected (e.g., hourly, daily). Should adaptive filtering or enrichment of feeds also be part of the solution?	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
499	Scope of Work and Technical Specifications	14	3.12.7	The bidder must analyze false positives and optimize detection algorithms.	Does NABARD expect MSSP to train TIP-based scoring logic using historical logs/incidents from the Bank? Will anonymized datasets or access to historical alerts be provided for this purpose?	Kindly refer to the RFP
500	Scope of Work and Technical Specifications	14	3.12.8	The bidder shall submit the following reports to Bank on a defined frequency a. Intelligence received (Daily) b. Incident report (Weekly, Monthly)	Please confirm if report formats/templates will be provided by NABARD or if bidder can use standard TIP reports. Should incident reports tie back to TIP-originated IOCs and threat clusters?	The report format shall be decided mutually between NABARD and the bidder.
501	Scope of Work and Technical Specifications	14	3.13..1	The bidder shall be responsible for supply, implementation, maintenance and support of SCM solution across the organization's endpoints /servers present in the Bank's infrastructure.	Please confirm if NABARD has any preferred SCM OEM or expects the MSSP to propose the complete stack. Also, is the SCM expected to be deployed as SaaS or on-prem?	Bidder has to provision a new SCM solution. Additionally, the solution should preferably be on-prem.
502	Scope of Work and Technical Specifications	14	3.13..2	The SCM solution shall be seamlessly integrated with the Bank's existing infrastructure devices and the proposed solutions such as AD, SIEM, Firewalls, Network devices, servers etc. The integration shall be carried out by the bidder.	Kindly share integration points or protocols (e.g., API, Syslog, SNMP, Agent-based) expected for SCM to interoperate with existing infra.	The same shall be shared with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
503	Scope of Work and Technical Specifications	14	3.13..3	The solution shall Provide real-time insights into compliance status, which allows organizations to quickly address any issues that arise	Please clarify if there is any regulatory framework baseline (e.g., RBI CSF, ISO 27001) that the real-time dashboard needs to reflect against.	Kindly refer to the RFP
504	Scope of Work and Technical Specifications	14	3.13..4	The solution shall perform automated compliance checks which Continuously monitors systems and processes to ensure they meet compliance requirements, reducing the risk of human error.	Please confirm if NABARD expects pre-defined compliance templates (e.g., for ISO, PCI-DSS, RBI CSF) or MSSP is expected to develop custom rule sets.	Templates may be defined by NABARD in consultation with the successful bidder.
505	Scope of Work and Technical Specifications	14	3.13..5	The solution shall Maintain detailed logs of compliance-related activities and generates reports for audits, helping demonstrate compliance to regulators and stakeholders.	Should the SCM solution include archival and log retention for a specific period (e.g., 5 years)? Should it be integrated with Bank's archival/log management system?	Yes
506	Scope of Work and Technical Specifications	14	3.13..6	The solution should Manage and enforce security policies across the organization, including updating policies as regulations change and ensuring all employees adhere to these policies.	Please confirm how MSSP is expected to enforce org-wide policies — whether via Group Policies, endpoint agents, or third-party tooling.	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
507	Scope of Work and Technical Specifications	15	3.13..7	The solution shall Include modules for training employees on compliance requirements and best practices.	Is the bidder expected to provide a full LMS-based training module or simply ensure OEM provides standard compliance training kits? Will NABARD host the LMS? Please confirm the number of Bank users expected to be trained.	Kindly refer to the RFP
508	Scope of Work and Technical Specifications	15	3.13..8	The solution shall generate reports: a. non-compliance reports (Daily, Weekly, Monthly)	Please confirm if report templates are defined by NABARD or if MSSP should provide standard dashboards and export formats. Should alerts be real-time for non-compliance cases?	Formats shall be finalised on mutual discussion between the successful bidder and NABARD.
509	Scope of Work and Technical Specifications	15	4.(b)	Bidder shall also allow NABARD to Audit/review the setup remotely and/or On Site by its own team and/or by any 3rd party Auditor appointed by NABARD on regular basis	Please confirm if NABARD will approve the audit scope or if bidder may propose it initially. Is the audit to be tool-focused or include the overall SOC process validation?	Kindly refer to the RFP

510	Scope of Work and Technical Specifications	15	5-a	The bidder along with the solution provided shall comply with the following standards: · Adherence to IT Act 2000 including 43 (A), MHA, CERT-In & LEA Guidelines issued by Govt, DPDP Act, RBI Guidelines. · Isolation of NABARD's digital and physical data path from other clients. · Compliance with the e-waste policies of relevant authorities and departments at the time of decommissioning any device, service or virtual machine. Only after verifying this compliance the hardware be handed over to the appropriate party. RBI Working group document on "Information Security, Electronic Banking, Technology Risk Management and Cyber Frauds" dated Jan 2011 RBI Cyber Security framework of June 2016 and its subsequent amendments RBI February 2021 Master Circular on Digital Payments security RBI circular on "Storage of Payment System Data" dated April 6, 2018 PA-DSS/PCI-DSS	Request clarification if bidder's tools must natively be certified (e.g., ISO 27001, SOC2) or compliance should be achieved through configurations and reports.	Compliance should be achieved through configurations and reports.

				guidelines/standards Data Privacy Guidelines Digital Personal Data Protection Act (DPDP) RBI's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices dt 07th November 2023 and latest amendments MITRE framework ISO 27001 framework SOC 2 Type II Any other relevant guidelines along with the subsequent amendments		

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
511	Scope of Work and Technical Specifications	16	5.(b)	Bidder must ensure robust protection against both internal and external threats, adhering to the principles of the Zero Trust security model.	Kindly elaborate on the scope of Zero Trust expected — is the MSSP required to deploy identity verification tools or just ensure policy-level enforcement in integration?	kindly refer to the RFP
512	Scope of Work and Technical Specifications	16	6.(a)	Bidder shall arrange the training for all proposed services/ tools by the OEMs proposed as part of the RFP. The topics should cover detailed functionality, configurations, troubleshooting etc of its product.	Please confirm the number of Bank users expected to be trained, duration per tool, and if remote trainings are allowed. Will NABARD define the training calendar per quarter?	Bidder has to arrange the training for a total of 20-30 NABARD officers. Mode of training may be decided mutually between NABARD and the bidder
513	Scope of Work and Technical Specifications	16	7.(a)	Bidder to Inform the bank of new patch upgrade for all security solutions on a quarterly basis.	Beyond informing, please clarify the MSSP's responsibility for planning, testing, and deploying these patch upgrades to all in-scope security solutions, including any associated downtime considerations.	In additional to intimation, bidder has to apply the patches on the tools provided by them in a timely manner.
514	Scope of Work and Technical Specifications	16	7.(c)	Complete lifecycle management activity shall govern for 5 years from Date of go-live	Please confirm if tools reaching End of Support (EOS/EOL) mid-contract can be replaced by functionally equivalent tools, and what is the approval process for such changes.	No tools shall reach the EOS/EOL within the contract period.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
515	Scope of Work and Technical Specifications	16	8.(a)	NABARD will review and discuss the performance during the first week of every month.	Please provide a template or list of key performance indicators (KPIs) and metrics that NABARD expects to be presented and discussed during these monthly review meetings.	The same shall be shared with the successful bidder.
516	Scope of Work and Technical Specifications	16	8.(d)	All review meetings will be held at NABARD's designated site.	1. Please confirm if hybrid (physical + remote) meetings will be permitted under special cases. 2. Should these be monthly per tool or consolidated at SOC level? Please confirm the cost of logistic support for the meeting will be borne by bidder or it will be NABARD responsibilty.	1. Kindly refer to corrigendum 2. Mechanism of review meeting shall be discussed with the successful bidder. However, no logistics cost shall be provided by NABARD.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
517	Payment Terms and Conditions	1	3	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 10% cost of the monthly contracted amount. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the monthly contracted amount even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor	Request NABARD to retain the capping to 5% of monthly contracted amount irrespective of the penalties under the individual towers.	Kindly refer to corrigendum
518	Project Timelines and Deliverables	1	1	Procure and supply solution components at DC, DR & Near site- T+ 1 Months	Bidder suggests that NABARD may go for pure MSSP services wherein all the responsibility of procurement / management/provision of services will lie with the bidder. If licenses are to be procured in the name of NABARD, then this should be a SI driven and OEM	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					led RFP which will be on CAPEX basis. But since NABARD is looking for "as a service" model, bidders suggests going for subscription model RFP.	
519	Service Level Agreement	13	10.1	Service Provider to offer training to NABARD's employees as defined in the RFP/GeM Bid on the software/hardware covering features, facilities, operations, implementation, trouble shooting, system administration, audit, MIS including report generation, etc.	Request NABARD to clarify whether the logistics of these training would be managed by NABARD or would it have to be accounted by the bidder. Also, the commercial bid makes no provision to include these costs. Request NABARD to add the relevant line items in the commercial bid.	The logistics of these training would be managed by bidder at no additional cost to NABARD

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
520	Non-Disclosure Agreement	5	1	In the event System Integrator is legally compelled to disclose any Confidential Information, System Integrator shall give sufficient notice of 45 days to NABARD to prevent or minimize to the extent possible, such disclosure. System Integrator shall disclose to third party i.e. any Confidential Information or the contents of this Agreement without the prior written consent of NABARD. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the System Integrator will apply to its own similar confidential information but in no event less than reasonable care. The obligations of this clause shall survive the expiration, cancellation or termination of this Agreement.	In the event System Integrator is legally compelled to disclose any Confidential Information, System Integrator shall **to the extent legally permissible,** give sufficient notice of 45 days to NABARD to prevent or minimize to the extent possible, such disclosure. System Integrator shall disclose to third party i.e. any Confidential Information or the contents of this Agreement without the prior written consent of NABARD. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the System Integrator will apply to its own similar confidential information but in no event less than reasonable care. The obligations of this clause shall survive the expiration, cancellation or termination of this Agreement.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
521	Non-Disclosure Agreement	6	6	Return of Confidential Information Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all the copies, abstracts, extracts, samples, notes, modules thereof to the Disclosing Party within seven (07) days after receipt of notice, and (iii) upon request of Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph.	Return of Confidential Information Upon written demand of the Disclosing Party, the Receiving Party shall (i) cease using the Confidential Information, (ii) return the Confidential Information and all the copies, abstracts, extracts, samples, notes, modules thereof to the Disclosing Party within seven (07) days after receipt of notice **(except to the extent it is legally entitled to retain)**, and (iii) upon request of Disclosing Party, certify in writing that the Receiving Party has complied with the obligations set forth in this paragraph.	No change
522	Non-Disclosure Agreement	7	7.5	Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.	Disclosing Party may visit Receiving Party's premises, with reasonable prior notice and during normal business hours, to review Receiving Party's compliance with the term of this Agreement.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
523	Service Level Agreement	10	6.1	If it is desired by NABARD/Reserve Bank of India or its regulators or any regulatory authority of the country, the Service provider shall subject themselves to an audit of the systems and processes followed by the Service Provider for the product supplied to NABARD as also the processes/services, by which, support is being provided to NABARD, including support services, escalation methodologies, change management processes, etc. as per the risk parameters finalized by the Bank/ such auditors.	If it is desired by NABARD/Reserve Bank of India or its regulators or any regulatory authority of the country, the Service provider shall subject themselves to an audit of the systems and processes followed by the Service Provider for the product supplied to NABARD as also the processes/services, by which, support is being provided to NABARD, including support services, escalation methodologies, change management processes, etc. as per the risk parameters finalized by NABARD the Bank/ such auditors.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
524	Service Level Agreement	10	6.2	The Service Provider shall, whenever required by such Auditors, furnish all relevant information , records/data to them. All costs for such audit shall be borne by the NABARD. No Audit or inspection will be allowed till Service Provider has received at least 5 business days' prior written notice for Audit or inspection conducted by NABARD, while prior notice may not be given for Audit or inspection conducted by Regulatory authority.	The Service Provider shall, whenever required by such Auditors, furnish all relevant information, records/data to them. All costs for such audit shall be borne by the NABARD. No Audit or inspection will be allowed till Service Provider has received at least 5 business days' prior written notice for Audit or inspection conducted **by Reserve Bank of India** or its regulators or any regulatory authority of the country NABARD, while prior notice may not be given for Audit or inspection conducted by Regulatory authority.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
525	Service Level Agreement	10	6.3	Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by the NABARD or in the certification submitted by the auditors, it is agreed upon by the Service Provider that it shall correct/ resolve the same within such timelines as prescribed by NABARD. The Service Provider shall provide certification of the auditor to NABARD regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies were observed.	Where any deficiency has been observed during audit of the Service Provider on the risk parameters finalized by the NABARD or in the certification submitted by the auditors, it is agreed upon by the Service Provider that it shall correct/ resolve the same within such timelines as prescribed by NABARD **at NABARD's cost**. The Service Provider shall provide certification of the auditor to NABARD regarding compliance of the observations made by the auditors covering the respective risk parameters against which such deficiencies were observed.	No change
526	Service Level Agreement	11	7.6	Upon receipt of advance notice of 3 (three) Business Days from NABARD, whether during the Term or thereafter, the Service Provider shall permit NABARD and/or its Authorized Representative(s) to, during normal business hours on any Business Day, access its premises	Upon receipt of advance notice of 3 (three) Business Days from NABARD, whether during the Term or thereafter, the Service Provider shall permit NABARD and/or its Authorized Representative(s) to, during normal business hours on any Business Day, access its	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				to inspect the electronic records maintained by the Service Provider in relation to the Project.	premises to inspect the electronic records maintained by the Service Provider in relation to the Project.	
527	Service Level Agreement	11	7.7	If required under Applicable Law, whether during the Term or thereafter, the Service Provider shall provide access to any Governmental Authority to inspect records, documents, books and accounts of the Service Provider maintained in relation to the Support Services rendered under this Agreement.	If required under Applicable Law, whether during the Term or thereafter, the Service Provider shall provide access to **RBI** any Governmental Authority to inspect records, documents, books and accounts of the Service Provider maintained in relation to the Support Services rendered under this Agreement.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
528	Service Level Agreement	13	11.3	Change Requests: Any change requests for applications would have to be first cleared by NABARD. After finalizing the proposed change, a Business Requirement Document(BRD) will be prepared followed by development, UAT testing and movement to production. The person day rate will remain the same during the project period and one year post the project period.	Change Requests: Any change requests for applications would have to be first cleared by NABARD. After finalizing the proposed change, a Business Requirement Document(BRD) will be prepared followed by development, UAT testing and movement to production. The person day rate will remain the same during the project period and one year post the project period.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
529	Service Level Agreement	18	18.2	Notwithstanding anything to the contrary contained anywhere in this Agreement, NABARD shall not be liable to the Service Provider for any pecial, consequential, incidental, exemplary, punitive, or indirect damages arising from, relating to, or in connection with this Agreement or any Schedules, Annexures or attachments hereto including, without limitation to, any damages resulting from loss of profits, loss of savings, loss of business, loss of use, or loss of data, arising out of or in connection with this Agreement or of any other obligations relating to this Agreement, whether or not the Party has foreseen or been advised of the possibility of such damages as well as for costs of procurement of substitute services by anyone.	Notwithstanding anything to the contrary contained anywhere in this Agreement, **neither Party** NABARD shall not be liable to the Service Provider for any special, consequential, incidental, exemplary, punitive, or indirect damages arising from, relating to, or in connection with this Agreement or any Schedules, Annexures or attachments hereto including, without limitation to, any damages resulting from loss of profits, loss of savings, loss of business, loss of use, or loss of data, arising out of or in connection with this Agreement or of any other obligations relating to this Agreement, whether or not the Party has foreseen or been advised of the possibility of such damages as well as for costs of procurement of substitute services by anyone.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
530	Service Level Agreement	22	22	INDEMNIFICATION 22.1. Service Provider shall indemnify and agrees to defend and to keep NABARD and its Affiliates and agents, officers, directors, employees successors and permitted assigns indemnified, from any and all Losses suffered arising from, or in connection with, any of the following: 22.1.1. the non-performance and non-observance of any of the terms and conditions of this Agreement by the Service Provider; 22.1.2. acts or omissions of the Service Provider which amount to negligence or willful misconduct; 22.1.3. any infringement or alleged infringement by the Service Provider of a Third Party's Intellectual Property; 22.1.4. any infringement or alleged infringement by the Service Provider of NABARD's Intellectual Property and/or Material 22.1.5. failure by the Service	INDEMNIFICATION 22.1. Service Provider shall indemnify and agrees to defend and to keep NABARD and its Affiliates and agents, officers, directors, employees successors and permitted assigns indemnified, from any and all Losses suffered arising from, or in connection with, any of the following: 22.1.1. the non-performance and non-observance of any of the terms and conditions of this Agreement by the Service Provider; 22.1.2. acts or omissions of the Service Provider which amount to **gross** negligence or willful misconduct; 22.1.3. any infringement or alleged infringement by the Service Provider of a Third Party's Intellectual Property; 22.1.4. any infringement or alleged infringement by the Service Provider of NABARD's Intellectual Property	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				Provider to fulfill its obligations under any applicable Law.	and/or Material 22.1.5. failure by the Service Provider to fulfill its obligations under any applicable Law.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
531	Service Level Agreement	24	23.2.1.(f)	23.2. Termination 23.2.1 Order Cancellation/ Termination of Contract f. If Service Provider fails to perform any other obligation(s) under the Contract.	23.2. Termination 23.2.1 Order Cancellation/ Termination of Contract f. If Service Provider fails to perform any other obligation(s) under the Contract.	No Change
532	Service Level Agreement	24	23.2.1.(g)	If Service Provider is not providing after sales and maintenance services and the calls are not attended for three or more occasions, NABARD is at liberty to terminate the Contract by giving 30 days' 'Notice'. If Service Provider provides remedy within 30 days of termination notice, NABARD may reconsider its decision of termination.	If Service Provider is not providing after sales and maintenance services and the calls are not attended for three or more occasions, NABARD is at liberty to terminate the Contract by giving 30 days' 'Notice'. If Service Provider provides remedy within 30 days of termination notice**, then the Notice stands cancelled.** NABARD may reconsider its decision of termination.	No change
533	Service Level Agreement	24	23.2.1.(j)	Termination in all circumstances will mean a proper transition with data transfer in a readable format along with all knowledge documents. Transition to take within a month unless extended by mutual consent.	Termination in all circumstances will mean a proper transition with data transfer in a readable format along with all knowledge documents. Transition to take	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					within a month unless extended by mutual consent.	
534	Service Level Agreement	25	23.2.2.(c)	Service Provider agrees that after completion of the Term or upon earlier termination of the Contract/assignment Service Provider shall, if required by NABARD, continue to provide warranty services to the NABARD at no less favorable terms than those contained in GeM Bid/Agreement. In case NABARD wants to continue with the Service Provider's service after the completion of this contract then Service Provider shall offer the same or better terms to NABARD. Unless mutually agreed, the rates shall remain firm.	Service Provider agrees that after completion of the Term or upon earlier termination of the Contract / assignment Service Provider shall, if required by NABARD, continue to provide warranty services to the NABARD at no less favorable terms than those contained in GeM Bid/Agreement. In case NABARD wants to continue with the Service Provider's service after the completion of this contract then Service Provider shall offer the same or better terms to NABARD. Unless mutually agreed, the rates shall remain firm.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
535	Service Level Agreement	25	23.2.2.(d)	NABARD shall make such prorated payment for services rendered by Service Provider and accepted by NABARD at the sole discretion of NABARD in the event of termination, provided that Service Provider 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 Service Provider.	NABARD shall make such prorated payment for services rendered by Service Provider to and accepted by NABARD at the sole discretion of NABARD in the event of termination, provided that Service Provider 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 Service Provider.	No change
536	Service Level Agreement	25	23.2.2.(e)	Notwithstanding the termination or expiry of this Agreement, all rights granted to NABARD pursuant to this Agreement shall survive.	Notwithstanding the termination or expiry of this Agreement, all rights granted to NABARD pursuant to this Agreement shall **survive till completion of the Reverse Transition Mechanism.**	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
537	Service Level Agreement	25	23.2.3	Termination of this Agreement (except as otherwise agreed to by the Parties) shall not release any Party hereto from any liability or obligation in respect of any matters, undertakings or conditions which shall have been done, observed or performed by that Party prior to such termination or which, at the said time has already accrued to the other Party. However, nothing herein shall affect, or be construed to operate as a waiver of, the right of any Party hereto aggrieved by any breach of this Agreement, to compensation for any injury or damages resulting therefrom which has occurred either before or after such termination.	Termination of this Agreement (except as otherwise agreed to by the Parties) shall not release any Party hereto from any liability or obligation in respect of any matters, undertakings or conditions which shall have been done, observed or performed by that Party prior to such termination or which, at the said time has already accrued to the other Party. However, nothing herein shall affect, or be construed to operate as a waiver of, the right of any Party hereto aggrieved by any breach of this Agreement, to compensation for any injury or damages resulting therefrom which has occurred either before or after such termination.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
538	Service Level Agreement	28	28.2	If the Service Provider fails to deliver any Support Services or meet any Service Levels under this Agreement, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' subject to maximum of 10% cost of the underperformed services. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the payments even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor.	If the Service Provider fails to deliver any Support Services or meet any Service Levels under this Agreement, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' subject to maximum of 10% cost of the underperformed services. However, **Liquidated Damages** Penalty under individual towers shall be added and overall **LD** penalty in this case may go above 10% of the payments even though the **LD** penalty under individual tower shall be restricted to 10%. In addition to the **LD** penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
539	Service Level Agreement	28	28.3	NABARD reserves the right to impose / waive any such liquidated damages. Parties agree that the liquidated damages constitute a genuine pre-estimate of the damages, losses, likely to be suffered by NABARD in the event of breach by the Service Provider of the terms hereof.	NABARD reserves the right to impose / waive any such liquidated damages. Parties agree that the liquidated damages constitute a genuine pre-estimate of the damages, losses **(not by way of penalty)**, likely to be suffered by NABARD in the event of breach by the Service Provider of the terms hereof.	No change
540	General	16	4.2 Dedicated Hosting model Point no.5	Entire Infra to be hosted in Tier IV equivalent Data Centre. Scope to remain the same as Co-located model above	Is it mandatory that the service provider should have Tier-4 Data centre? Or it is ok to have Tier-3 Data centre?	The referred clause is not a part of the RFP
541	General	16	4.2 Dedicated Hosting model Point no.6	Virtualization provided by the respondent as part of solution shall be compatible with NABARD's present and future hosting requirements.	Which virtualized platform will be require to host the set-up?	The referred clause is not a part of the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
542	General	16	4.3 Infrastructure as a Service (Iaas) model Point no.1	The model may include both Private Cloud as well as Sovereign cloud as the case may be.	Here, does the bidder has to provide dedicated private cloud? Or bidder can host the infrastructure on their shared cloud platform? Tata Communications does have IZO Private Cloud solution which is MeiTY empanelled	The referred clause is not a part of the RFP
543	General	23	Appendix II, IaaS Point no.1	Compute, storage, networks, backups, security and other fundamental resources to be provided where NABARD and associated vendors are able to deploy and run the ERP software using control panel.	Is it ok for bidder to provide the complete Cloud hosting infra on shared environment (Compute, Storage, Backup)? Tata Communications does have IZO Private Cloud solution which is MeiTY empanelled	The referred clause is not a part of the RFP
544	General	23	Appendix II, IaaS Point no.2	Service provider shall be responsible for managing and controlling the underlying virtualized infrastructure including storage, network, security, etc. and the deployed applications shall be managed and controlled by NABARD and its associated vendors.	Does customer have specific virtulization platform requirements? Tata Communications have IZO Private Cloud which built on Vmware ESXi platform.	The referred clause is not a part of the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
545	General	23	Appendix II, IaaS Point no.6	The Service shall provide auto-scalable, redundant, and dynamic computing capabilities	Please specify which servers will require auto-scaling feature? TCL requests customer to provide required scalable sizing to map the Virtual machine for future readiness.	The referred clause is not a part of the RFP
546	General	23	Appendix II, IaaS Point no.8	Respondent shall allow users to securely and remotely, load applications over the SSL VPN clients from the public internet.	Please provide details about required Internet BW, Client to Site and Site to Site VPN connection count.	The referred clause is not a part of the RFP
547	General	23	Appendix II, IaaS Point no.9	Perform an Image backup of VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into NABARD's required format.	Tata Communications offers periodic backup solution. As per the customer's requirement, our team will configure schueduled backup.	The referred clause is not a part of the RFP
548	General	14	3.4 IT Infrastructure	Dedicated SOC and NOC – SOC to be run by different vendors in order to avoid conflict of interest	What is the difference between dedicated SOC and NOC-SOC.	The referred clause is not a part of the RFP
549	General	14	3.4 IT Infrastructure	Dedicated SOC and NOC – SOC to be run by different vendors in order to avoid conflict of interest	Annexure IV for which SOC? Dedicated SOC or NOC-SOC	The referred clause is not a part of the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
550	General	25	Appendix IV - SOC Requirements	Intrusion Detection and Prevention Systems (IDPS): These tools are used to detect and prevent attacks against the network infrastructure.	IDPS will be part of Firewall. Hence request NABARD to remove it from scope of SOC	The referred clause is not a part of the RFP
551	General	25	Appendix IV - SOC Requirements	Endpoint Security Tools: These tools are used to protect endpoints, such as laptops, desktops, and mobile devices, from security threats.	Are the endpoint security solutions in place and need to be integrated with the SOC? If yes, please share the list of technologies	The referred clause is not a part of the RFP
552	General	25	Appendix IV - SOC Requirements	Endpoint Security Tools: These tools are used to protect endpoints, such as laptops, desktops, and mobile devices, from security threats.	If No, Please let us know the count of endpoints (desktops/laptops/Mobile devices) which need to be covered under this scope. Also, please mention the technologies that need to be covered for these endpoints	The referred clause is not a part of the RFP
553	General	25	Appendix IV - SOC Requirements		Is NABARD comfortable with a multitenant Cloud SOC or is there a need to deploy a dedicated SIEM solution	The bidder has to deploy the dedicated SIEM tool.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
554	Scope of Work and Technical Specifications	1	2.(a)	The bidder must deliver managed security services for NABARD, ensuring that the entire solution is deployed at NABARD designated locations on pay-as-you-go model. This approach aims to ensure that NABARD's infrastructure is both secure and scalable, meeting the organization's evolving needs over the contract period.	In case of NABARD opting for pay-as-you-go model, licenses would typically owned by service provider only. Kindly confirm if NABARD is agreeing with this	Kindly refer to the RFP
555	Scope of Work and Technical Specifications	4	(y)	Licenses for the entire project may be procured in the name of the vendor or NABARD. However, any such arrangements should not violate the licensing policy of any OEM. The service provider shall be liable for any punitive action or damage for violation of licensing policies	In case of NABARD opting for pay-as-you-go model, licenses would typically owned by service provider only. Kindly confirm if NABARD is agreeing with this	Kindly refer to the RFP
556	Payment Terms and Conditions	1	2	Payment shall be made on a quarterly basis, in arrears	Request to change billing frequency to Quarterly in Advance. Payment terms will be Net 30 days from date of invoice.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
557	Payment Terms and Conditions	1	3	If the Service Provider fails to deliver any Support Services or meet any Service Levels, NABARD shall be entitled to liquidated damages as specified under Schedule 'A' of the SLA subject to maximum of 10% cost of the monthly contracted amount. However, Penalty under individual towers shall be added and overall penalty in this case may go above 10% of the monthly contracted amount even though the penalty under individual tower shall be restricted to 10%. In addition to the penalty, proportionate payment for the downtime except for approved downtime shall not be made to the vendor	Request to cap the overall penalty to 10%	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
558	Scope of Work and Technical Specifications	1	1.(a) and 1.(b)	1.(a) The RFP seeks to engage a Managed Security Service Provider (MSSP) for providing managed SOC services across the proposed Bank's Infrastructure which consists of Private Cloud spanning across DC, DR and near Site. This includes the procurement of necessary hardware and related tools, as well as the ongoing operations and management of the entire Security solution. The entire solution has to be maintained over a five-year period from the go live date. NABARD may further extend the contract beyond a term of 5 years on a mutual agreement basis. 1.(b) The solution will be procured on an operational expenditure (Opex) basis, ensuring high availability and allowing for a rate contract to accommodate any additional or	Kindly confirm if hardware need to be supplied by bidder. In this case opex model of payment need clarity. Whether it is for only software and manpower	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				enhanced requirements as they arise.		
559	Project Timelines and Deliverables	1	2	Kindly confirm if hardware need to be supplied by bidder. In this case opex model of payment need clarity. Whether it is for only	In case of deployment of hardware infrastructure, this timeline may not be feasible	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				software and manpower- T+45 Days		
560	Service Level Agreement	37	3.1	SLAs for Security Solutions viz. SIEM, SOAR, WAF, DAM, SWG, PAM, EDR, EASM, TIP, SCM, NBAD on individual basis	Request SLA to be modified to 98%	No change

561	QCBS Evaluation Criteria	2	B.(1)	Experience in providing Managed SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 4 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22, 2020-21 (Bidder shall submit PO/credential letters) a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks Further, the bidder shall submit the customer's feedback form having positive feedback, as attached in Annexure I, against the submitted PO/credential letters and the marks allocated against the same are as below: a) 02 projects - 3 Marks b) 03 projects - 4 Marks c) 04 projects - 5 Marks Additionally, if the submitted POs as per the above criteria pertain to the BFSI clients, additional marks as below shall be allocated a) 03 to 05 projects - 3 Marks	1. Request you to change to below Experience in providing Managed/Captive SOC service for the client similar to the Scope of Work of this RFP/GeM Bid with a minimum of 2 solutions/tools proposed in the RFP in which SIEM with a minimum of 10k EPS and SOAR are compulsory in last 5 years. (FY 2024-25, 2023-24, 2022-23, 2021-22, 2020-21 (Bidder shall submit PO/credential letters) a) 03 to 05 projects - 3 Marks b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks 2. Request you to change to below Further, the bidder shall submit the Customer feedback /customer signoff document form having positive feedback, as attached in Annexure I, against the submitted PO/credential letters and the marks allocated against the same are as below: a) 02 projects - 3 Marks	No Change

				b) 06 to 07 projects - 4 Marks c) 08 projects and above - 5 Marks	b) 03 projects - 4 Marks c) 04 projects - 5 Marks	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
562	QCBS Evaluation Criteria	2	B.2.(A)	The proposed SIEM solution with a minimum of 10000 EPS should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 7 marks (b) 13 to 14 references -5 marks (c) 10 to 12 references- 3 marks	Request you to change to below The SIEM solution with a minimum of 10000 EPS should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 8 references and above- 7 marks (b) 5 references and above -5 marks (c) 3 references and above- 3 marks	Kindly refer to corrigendum
563	QCBS Evaluation Criteria	2	B.2.(B)	The proposed SOAR + TIP solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b)(b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Request you to change to below The proposed SOAR + TIP solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 2023-2024, FY 2024-2025): Service Experience: (a) 15 references and above- 4	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	
564	QCBS Evaluation Criteria	3	B.2.(C)	The proposed WAF solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Request you to change to below The proposed WAF solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
565	QCBS Evaluation Criteria	3	B.2.(D)	The proposed DAM solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Request you to change to below The proposed DAM solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Kindly refer to corrigendum
566	QCBS Evaluation Criteria	3	B.2.(E)	The proposed SWG solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Request you to change to below The proposed SWG solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					(c) 10 to 12 references- 2 marks	
567	QCBS Evaluation Criteria	3	B.2.(F)	The proposed PAM solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Request you to change to below The proposed PAM solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
568	QCBS Evaluation Criteria	3	B.2.(G)	The proposed EDR solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	The proposed EDR solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks	Kindly refer to corrigendum
569	QCBS Evaluation Criteria	3	B.2.(H)	The proposed EASM solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 3 marks (b) (b) 13 to 14 references -2 marks (c) 10 to 12 references- 1 marks	Request you to change to below The proposed EASM solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 3 marks (b) (b) 13 to 14 references -2 marks (c) 10 to 12 references- 1 marks	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
570	QCBS Evaluation Criteria	4	B.2.(I)	The proposed SCM solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 3 marks (b) 13 to 14 references -2 marks (c) 10 to 12 references- 1 marks	Request you to change to below The proposed SCM solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 3 marks (b) 13 to 14 references -2 marks (c) 10 to 12 references- 1 marks	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
571	QCBS Evaluation Criteria	4	B.2.(J)	The proposed NBAD solution with should have been supplied and implemented by OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 15 references and above- 4 marks (b) 13 to 14 references -3 marks (c) 10 to 12 references- 2 marks OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices/signoff Letter.	Request you to change to below The proposed NBAD solution with should have been supplied and implemented by Bidder/OEM in India in last five years (FY 2020-2021, FY2021-2022, FY2022-2023, FY 20232024, FY 2024-2025): Service Experience: (a) 3 references and above- 4 marks (b) 2 references -3 marks (c) 1 references- 2 marks OEM should provide completion certificate/ reference letter email from client along with the copy of purchase order/ contract agreement/ work order/ engagement letter/ invoices/signoff Letter.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
572	QCBS Evaluation Criteria	4	D	The bidder must have IT Security resources on permanent payroll having experience in-scope solutions with Certifications such as CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH (a) 50 to 75 resources- 04 marks (b) 76 and above resources- 09 marks Note: (i) Resources for CEH- Max 10 resources will be considered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource has more than one certification, it will be considered as one. (iii) Of the above, the bidder must have a total of 5 certified resources of the proposed SIEM solution on permanent payroll. If not, then the count of resources will not be considered, and no marks shall be awarded under Clause 'D'.	Request you to change to below The bidder must have IT Security resources on permanent payroll having experience in-scope solutions with Certifications such as CISSP/CISSP IS2/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH /ISO /CCNP/CCNP security/CompTIA security + (a) 50 to 75 resources- 04 marks (b) 76 and above resources- 09 marks Please remove CEH MAX 10 resources criteria	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
573	Minimum Eligibility Criteria	2	7	Experience a) The bidder should have experience of providing managed security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024-25, FY 2023-24, 2022-23, 2021-22, 2020-21). b) Of the above submitted POs, at leastone (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches (This shall override experience criteria given in the bid in other documents)	Request you to change to below Experience a) The bidder should have experience of providing managed /Captive security services with minimum 4 solutions, mandatorily consisting of proposed SIEM with minimum of 10k EPS and SOAR, and any 2 among proposed PAM, EDR, NBAD, DAM, WAF, SWG, TIP, SCM, EASM) for atleast 3 distinct clients in the last 5 years (FY 2024-25, FY 2023-24, 2022- 23, 2021-22, 2020-21). b) Of the above submitted POs, at leastone (1) PO should be of a Schedule Commercial Bank in India having more than 1000 branches (This shall override experience criteria given in the bid in other documents)	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
574	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/OSCP/ CEH certified. Note: (i) Resources for CEHMax 10 resources shall be considered. The certification date must be prior to the date of publication of this RFP.	Request you to consider below : CISSP/CISSP IS2/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH /ISO /CCNP/CCNP security/CompTIA security + Please remove CEH MAX 10 resources criteria	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				(ii) If a resource is carrying more than one certification, it shall be considered as one.		

575	BOM and Commercials	1	10	NBAD as a service- 5000 FPS	1. Request you to change to 5000 FPS/Packets per second 2. For a packet-based NBAD Solution, we request to consider NBAD Solution at each site (DC, DR, and NDR) to be capable of handling respective throughputs with 5 days of packet-level data storage for back-in-time investigation, forensics, host investigation, session analysis, and packet analysis. Secondly, with a sampling rate of 1:1, for 1Gbps of traffic, NBAD Solution is required to support 100 K FPS. For security solutions like NBAD, we need to have 1:1 sampling and active timer of 120 seconds. Please confirm what the traffic throughput is in each site DC, DR, and NDR, and accordingly we recommend the FPS in this point to be resized considering a sampling rate of 1:1 and active timer 120 seconds. 3. The Commercial Format and technical specifications of NBAD Solution are completely NetFlow-based; this will limit	Kindly refer to the revised BOM and Commercials Format

					participation of OEMs who can deliver the NBAD functionality with other technologies, like packet-based. We request Bank confirm if they are willing to consider a packet-based NBAD solution; if yes, then multiple other technical specifications need to be amended to accommodate both NetFlow and packet-based NBAD solutions.	
576	GeM Bid Document	2		EMD- SBI	request you to kinldy consider EMD from leading private Bank	Kindly refer to the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
577	GeM Bid Document	2		ePBG- SBI	request you to kinldy consider PBG from leading private Bank	Kindly refer to the RFP
578	General			Additional Point	Hardware will be provided by NABARD Please confirm	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.
579	Scope of Work and Technical Specifications	41	15	The solution should have authentication options for users/groups. It should supports authentication of users via Integrated Windows Authentication, NTLM (NTLM v1 and v2 in Session Security), and LDAP.	Request to change clause as - The solution should have authentication options for users/groups. It should supports authentication/identifications of users via (Integrated Windows Authentication),LDAP synchronization or SAML based authentication.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
580	General			Additional Point	if Cloud Native,the Cloud Native vendor must have atleast 8 Datacenters across 5 different zones in India region with SLA of 99.999%	No Change
581	General			Additional Point	The proposed data centre must be certified with ISO27017, ISO27018 and solution should be SOC2-Type II compliant.1 mark for ISO27017 and ISO27018, 1 mark	No Change
582	General			Additional Point	The vendor must provide SLA for decrypted traffic, committing to less than or ~ 60 ms to 125 ms latency for processing encrypted traffic to ensure better performance while accessing applications and better end user experience.	No Change
583	Service Level Agreement	10	6	Audit Services	The scope, periodicity of Audit should be agreed between the parties.	Kindly refer to the RFP
584	Service Level Agreement	18	18	Limitation of Liability	Liability of the Service Provider should be limited to 12 months of charges received from customer under a specific purchase order giving rise to a liability. Niether of the parties	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					should be liable for any idirect and consequential damages under the RFP.	
585	Service Level Agreement	22	22	Indemnification	Service Provider shall only indemnify customer for willful misconduct, gross negligence, damage to tangible property or death, indemnity should be subject to limitation of liabilty i.e.12 months of charges received from customer under a specific purchase order giving rise to a liability	No change
586	Service Level Agreement	23	23.2	Termination	Customer should terminate only in case of material breach by the Service Provider and if Service Provider fails to rectify the breach within 90 days. In case of early termination by Customer, the Customer shall be liable to pay early termination charges.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
587	BOM and Commercials	2	10	NBAD as a service - Per 500 FPS	The Commercial Format and technical specifications of NBAD Solution are completely NetFlow-based; this will limit participation of OEMs who can deliver the NBAD functionality with other technologies, like packet-based. We request Bank confirm if they are willing to consider a packet-based NBAD solution; if yes, then multiple other technical specifications need to be amended to accommodate both NetFlow and packet-based NBAD solutions.	Kindly refer to the revised BOM and Commercials Format
588	Scope of Work and Technical Specifications	13	3.11	NBAD as a services Scope of work	Traffic Usage in FPS is for NetFlow-based NBAD Solution; this will limit participation of OEMs who can deliver the NBAD functionality with other technologies, like packet-based. We request Bank to confirm if they are willing to consider a packet-based NBAD solution; if yes, then this point needs to be changed to "Traffic Usage in FPS or bps or pps (Daily)"	Bidder can either propose flow based or packet based NBAD solution.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
589	Scope of Work and Technical Specifications	70	45	The solution should perform analysis on network data all the way up to the Layer 7 and provide complete application visibility	Layer 7/Application visibility can be achieved with a packet-based NBAD solution that utilizes deep packet inspection technology for a comprehensive application visibility; a Netflow-based solution depends on the Layer 3/4 information that does not provide complete Layer 7/Application visibility. So, we request Bank confirm if they are willing to consider a packet-based NBAD solution; if yes, then multiple other technical specifications need to be amended to accommodate both NetFlow and packet-based NBAD solutions.	Kindly refer to corrigendum
590	Scope of Work and Technical Specifications	68	2	The NDR/NBAD tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NDR/NBAD integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.	We request to include hostname and amend this point as follows: The NDR/NBAD tool should provide the internal network visibility and actionable insight required to quickly identify the threats. Additionally, NDR/NBAD integrates user or hostname information with	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.	
591	Scope of Work and Technical Specifications	68	3	The NDR /NBAD solution should also offer the flexibility and capability to drill down into the end user, MAC, flows, interface utilization and a wide array of other host statistics needed for rapid incident resolution. Should utilize anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration. The Solution should be able to detect Malwares on both encrypted and nonencrypted payloads.	We request to amend this point as follows: The NDR /NBAD solution should also offer the flexibility and capability to drill down into the end user or hostname or MAC, flows or packet, interface or application or server or host utilization and a wide array of other host statistics needed for rapid incident resolution. Should utilize anomaly detection methods to identify attacks such as zero-day exploits, self-modifying malware, attacks in the ciphered traffic or resource misuse or misconfiguration. The Solution	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					should be able to detect Malwares on both encrypted and nonencrypted payloads.	
592	Scope of Work and Technical Specifications	68	6	Network Detection and Response (NDR)/NBAD solutions take advantage of the flow technologies built into network devices. NDR /NBAD tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs data into meaningful analytics data like numbers charts and tables that quantify exactly how the network is being used, by whom and for what purpose.	We request to amend this point as follows: Network Detection and Response (NDR)/NBAD solutions take advantage of the flow or packet technologies built into network devices. NDR /NBAD tools should be able to capture data from continuous streams of real time network traffic and convert those raw logs or packet data into meaningful analytics data like numbers charts and tables that	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					quantify exactly how the network is being used, by whom and for what purpose.	
593	Scope of Work and Technical Specifications	68	7	Unsupervised and supervised machine learning along with probabilistic mathematics without predefined rules and signatures should be employed by the solution to detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack	We request to amend this point as follows: Unsupervised and supervised machine learning along with probabilistic mathematics, or multi-dimensional and deterministic ML techniques should be employed by the solution to detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
594	Scope of Work and Technical Specifications	68	9	NDR/NBAD solution should be able to use the existing network environment as a sensor grid to analyse traffic flow across the across the existing network and security solutions in a non-disruptive manner	We request to amend this point as follows: NDR/NBAD solution should be able to use the existing network environment as a sensor grid to analyse traffic flow or packets across the existing network and security solutions in a non-disruptive manner	Kindly refer to corrigendum
595	Scope of Work and Technical Specifications	69	10	The solution should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.	We request to amend this point as follows: The solution should allow either manually or via an automated discovery function to identify/add network devices and capture information such as IP address, OS, services provided, other connected hosts.	Kindly refer to the clause number 44 of the RFP

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
596	Scope of Work and Technical Specifications	69	13	The system should be able to monitor flow data between various VLANs.	We request to amend this point as follows: The system should be able to monitor flow or packet data between various VLANs.	Kindly refer to the clause number 57 of the RFP
597	Scope of Work and Technical Specifications	69	14	The solution should have the capability of application profiling in the system and also support custom applications present or acquired by the end user.	We request to amend this point as follows: The solution should have the capability of application profiling or host baselining in the system and also support custom applications present or acquired by the end user.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
598	Scope of Work and Technical Specifications	69	15	The solution should have the capability to enrich flow records with additional fields including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, number of packets and number of bytes transmitted in a session, timestamps for start and end of session, NAT translations, etc. from captured data and then utilize those fields in analytical algorithms to alarm on anomalous behaviour's.	We request to amend this point as follows: The solution should have the capability to enrich flow records or packet level data with any of the fields like source and destination IPs, source and destination MAC address or hostname, TCP/UDP ports or ICMP types and codes, number of packets and number of bytes transmitted in a session, timestamps for start and end of session, NAT translations, etc. from captured data and then utilize those fields in analytical algorithms to alarm on anomalous behaviour's.	No change
599	Scope of Work and Technical Specifications	69	16	The solution must be able to track user's activities locally and remote network sites and should be able to report usage behaviour across the entire network.	We request to amend this point as follows: The solution must be able to track user's or host activities locally and remote network sites and should be able to report usage behaviour across the entire network.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
600	Scope of Work and Technical Specifications	69	17	The solution should support all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.	We request to amend this point as follows: The solution should support security analytics using either packet-level data or all forms of flows including but not limited to Netflow, IPFIX, sFlow, Jflow, cFlowd, NSEL.	Kindly refer to corrigendum
601	Scope of Work and Technical Specifications	69	18	The solution should be able to combine/stitch the flow records coming from different network devices like routers, switches, firewalls that are associated with a single conversation and present them as a single bi-directional flow record.	This is a Netflow specific feature, so request to delete this point.	Kindly refer to corrigendum
602	Scope of Work and Technical Specifications	69	19	The solution must be able to stitch flows into conversations even when the traffic is NATed by the firewall; clearly showing the original and translated IP address.	This is a Netflow specific feature, so request to delete this point.	Kindly refer to corrigendum
603	Scope of Work and Technical Specifications	69	23	The system should provide detailed visibility to identify devices/servers/subnet information within a network automatically.	We request to amend this point as follows: The system should provide detailed visibility to identify devices/servers/subnet	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					information within a network automatically or manually.	
604	Scope of Work and Technical Specifications	69	27	The solution should provide the capability to define custom policies to evaluate flow attributes such as byte ratios, services, process, name and more.	We request to amend this point as follows: The solution should provide the capability to define custom policies to evaluate flow attributes such as byte ratios, services, process, name and more, or packet data such as source/destination IP, protocol, application, etc.	No change
605	Scope of Work and Technical Specifications	70	33	The solution shall use behavioural technology and machine learning and advanced entity modelling to reduce false positives. Solution should detect significant anomalies and drifts in user, device or network activities and traffic that signal an attack.	We request to amend this point as follows: The solution shall use multi-dimensional and deterministic ML techniques, or behavioural technology and machine learning and advanced entity modelling to reduce false positives. Solution should detect significant anomalies and drifts in user, device, host or network	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					activities and traffic that signal an attack.	
606	Scope of Work and Technical Specifications	70	34	The solution should use a mathematical modelling to create statistically significant views of user, device and network behaviours and detecting attacks that are already within the enterprise.	We request to amend this point as follows: The solution should use multi-dimensional and deterministic ML techniques, or a mathematical modelling to create statistically significant views of user, device, host or network behaviours and detecting attacks that are already within the enterprise.	No Change
607	Scope of Work and Technical Specifications	70	37	The solution should automatically learn a normal pattern of life for every user, device and network and is capable of detecting the most subtle cyber- threats within the network, including insider threat.	We request to amend this point as follows: The solution should automatically learn a normal pattern of life for every user, host, device or network and is	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					capable of detecting the most subtle cyber- threats within the network, including insider threat.	
608	Scope of Work and Technical Specifications	70	41	The solution should produce detailed visibility to identify devices/servers/subnet information within a network automatically.	We request to amend this point as follows: The solution should produce detailed visibility to identify devices/servers/subnet information within a network automatically or manually.	No Change
609	Scope of Work and Technical Specifications	71	53	The solution should be able to analyse SMTP traffic to detect high volume email, abnormal patterns in email traffic, traffic from unfriendly countries and with character sets often used by attackers (ex. Chinese).	We request to amend this point as follows: The solution should be able to analyse SMTP traffic to detect anomalies in email traffic or traffic from unfriendly/unexpected countries.	No change
610	Scope of Work and Technical Specifications	71	54	The solution should support execution of rules for historical traffic metadata.	We request to amend this point as follows: The solution should support execution of rules for historical	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					traffic metadata, or threat hunting using host investigation, session analysis or packet analysis.	
611	Scope of Work and Technical Specifications	71	60	The solution must support VPN tunnel detection for private and anonymous VPN tunnels and just not the VPN used by the Organization. Privacy VPN - Personal VPN solutions which enable the user to avoid network monitoring solutions.	We request to amend this point as follows: The solution must support features like Protocol tunneling or VPN tunnel detection for private and anonymous VPN tunnels and just not the VPN used by the Organization. Protocol Tunneling methods or Privacy VPN - Personal VPN solutions which enable the user to avoid network monitoring solutions.	No Change
612	Scope of Work and Technical Specifications	71	61	The solution should support extraction of documents, images, binary data, etc. and allow for similar documents, etc. to be discovered using simple search.	We request to amend this point as follows: The solution should support detection or extraction of malicious documents, images, binary data, etc. and allow for similar documents, etc. to be discovered using simple search.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
613	Scope of Work and Technical Specifications	71	63	NDR/NBAD solution should provide a full-featured Network threat analyser capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow analysis techniques and the ability to detect deviations from normal baselines.	We request to amend this point as follows: NDR/NBAD solution should provide a full-featured Network threat analyser capability to detect threats emerging from inside the network (i.e., ones that have not passed through a perimeter FW/IPS). This includes the ability to establish “normal” traffic baselines through flow or packet analysis techniques and the ability to detect deviations from normal baselines.	Kindly refer to corrigendum
614	Scope of Work and Technical Specifications	72	66	The solution should detect events of denial-of-service (DoS) and distributed denial of- service (DDoS) attacks including network flood events of ICMP, UDP, TCP SYN, TCP NULL, IP NULL, identify the presence of botnets in the network, etc. and detect long-lived connections that may be associated with data-exfiltration.	We request to amend this point as follows: The solution should detect attack vectors, IOCs, etc., associated with denial-of-service (DoS) and distributed denial of-service (DDoS) attacks including network flood events of ICMP, UDP, TCP SYN, TCP NULL, IP NULL, identify the presence of botnets in the network, etc. and	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					detect long- lived connections that may be associated with data-exfiltration.	
615	Scope of Work and Technical Specifications	72	68	The solution must be able to provide visibility of user endpoint workstations and support & service options to collect telemetry from these endpoints including username, process names and process hashes involved in the network traffic. If there is any License to be provided, the same should be considered for 50 endpoint workstations from day one.	We request to amend this point as follows: The solution must be able to provide visibility of user endpoint workstations or hostname and support & service options to collect telemetry from these endpoints like username, process names, process hashes or hostname involved in the network traffic. If there is any License to be provided, the same should be considered for 50 endpoint workstations from day one.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
616	Scope of Work and Technical Specifications	73	81	The solution should integrate with Open LDAP, Microsoft Active Directory, RADIUS and DHCP to provide user Identity information in addition to IP address information throughout the system & allow groups based on Identity or Active	We request to amend this point as follows: The solution should integrate with Open LDAP, Microsoft Active Directory, RADIUS, DHCP or DNS to provide user Identity information like hostname in addition to IP address information throughout the system & allow groups based on Identity or Active	No change
617	Scope of Work and Technical Specifications	73	82	Directory workgroup & provides full historical mapping of Username to IP address logins in a searchable format.	We request to amend this point as follows: Directory workgroup or Hostname & provides full historical mapping of Username or hostname to IP address in a searchable format.	No change
618	Scope of Work and Technical Specifications	73	98	The solution should have capability to categorize hosts into logical groups by observing traffic to achieve smarter segmentation. Admin may confirm, exclude or ignore any suggestion based on the network architecture.	We request to amend this point as follows: The solution should have capability to categorize hosts into logical groups either manually or by observing traffic to achieve smarter	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					segmentation. Admin may confirm, exclude or ignore any suggestion based on the network architecture.	
619	Scope of Work and Technical Specifications	73	99	The solution should have an automated scanner to identify assets and should also be able to schedule the scans	We request to amend this point as follows: The solution should have either have an automated scanner to identify assets and should also be able to schedule the scans or manually add hosts to logical asset groups for policy based violations.	Kindly refer to corrigendum
620	Scope of Work and Technical Specifications	73	102	The solution should have detailed ASN traffic visibility	This is a Netflow specific feature, so request to delete this point.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
621	Scope of Work and Technical Specifications	13	3.11.2	The NBAD solution shall be seamlessly integrated with the Bank's existing infrastructure and network devices and the proposed solutions such as AD, SIEM, Firewalls etc. The integration shall be carried out by the bidder.	We request to amend this point as follows: The NBAD solution shall be seamlessly integrated with the Bank's existing infrastructure and network devices and the proposed solutions such as AD or DNS, SIEM, Firewalls etc. The integration shall be carried out by the bidder.	No change
622	Scope of Work and Technical Specifications	15	5.(a)	The bidder along with the solution provided shall comply with the following standards	The proposed solution has been deployed across multiple BFSI enterprises in India. However, as indicated in the compliance section, any written confirmation of the stated standards can be a challenge. Hence, we request to define key potential desirable features and capabilities of the solution.	No change
623	Scope of Work and Technical Specifications	4	(ii)	All the tools proposed by the bidder must be in High Availability mode ensuring redundancy.	The proposed Packet-based NBAD Solution will have a Management Console in High Availability, hope this is acceptable.	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
624	Scope of Work and Technical Specifications	73	94	The solution must be deployed in Centralized mode with central management and reporting from the single dashboard for the entire deployment.	Please confirm if NABARD will provide a VM for Centralized Management Console.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.
625	Scope of Work and Technical Specifications	1	1.(a)	The RFP seeks to engage a Managed Security Service Provider (MSSP) for providing managed SOC services across the proposed Bank's Infrastructure which consists of Private Cloud spanning across DC, DR and near Site.	1. Please confirm if NBAD Solution is expected to monitor traffic inside a Private Cloud. 2. Please clarify the type (copper/fibre) and speed (1G, 10G, 25G, 40G, 100G) of network ports used in NABARD network. This is required for sizing the NBAD Solution.	The same shall be shared with the successful bidder.

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
626	Scope of Work and Technical Specifications	61	38	Solution should have the ability to allow users to customize the weight of incidents in their overall risk score based on the organizations needs	At present, customization of the risk score by the customer is not supported. However, the CloudSEK platform is built on an AI/ML-driven engine that automatically prioritizes risks based on severity levels — High, Medium, and Low. Additionally, incidents can be classified as False Positive, Informational, or Irrelevant, and based on these classifications, they can be assigned to the respective team members for appropriate action.	No change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
627	Scope of Work and Technical Specifications	1	1.(a)	The RFP seeks to engage a Managed Security Service Provider (MSSP) for providing managed SOC services across the proposed Bank's Infrastructure which consists of Private Cloud spanning across DC, DR and near Site. This includes the procurement of necessary hardware and related tools, as well as the ongoing operations and management of the entire Security solution. The entire solution has to be maintained over a five-year period from the go live date. NABARD may further extend the contract beyond a term of 5 years on a mutual agreement basis	The packet-based NBAD Solution may require certain physical appliances to be installed in the NABARD Infrastructure. This depends on the traffic volume/throughput to be inspected. For higher traffic volume, physical appliances are recommended. Please clarify if we can propose physical appliances if needed to handle higher traffic volume.	NABARD shall be providing the virtual machines over which the vendor has to deploy their tools. However, for tools not feasible to be deployed on VMs, the SaaS based offering may be considered subject to Data sovereignty and residency clauses. No physical device based solution shall be proposed for the setup. Additionally, all the tools deployed shall be in active-active mode at all the sites.
628	General			Additional Point	TIP – Bidder should have atleast two commercials feeds and 25+ open source feeds	No Change
629	General			Additional Point	In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
630	Scope of Work and Technical Specifications	11	3.8	External Attack Surface Monitoring (EASM) as a service	Perform attack surface assessment of third-party vendors / service providers.	Kindly refer to the RFP
631	Project Timelines and Deliverables	1	1	Procure and supply solution components at DC, DR & Near site- T+1 Months	Typical delivery time is 6 to 8 weeks, so we request to change this point as follows: Procure and supply solution components at DC, DR & Near site T+ 2 Months	No change
632	Minimum Eligibility Criteria	1	1	Legal Entity The bidder should be a government organization / Public sector unit/Partnership firm / Limited Company / Private Limited Company /Limited Liability Partnership / Private or Public Listed Company. Further, the bidder should be a legal entity formulated / registered in India under applicable acts/laws for more than 3 years as on 31.03.2025.	Legal Entity The bidder should be a government organization / Public sector unit/Partnership firm / Limited Company / Private Limited Company / Limited Liability Partnership / Private or Public Listed Company. Further, the bidder should be a legal entity formulated / registered in India under applicable acts/laws for more than 3 years as on 31.03.2025 or	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					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 5 years as on the date of submission of bid.	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
633	Minimum Eligibility Criteria	1	2	Financials a. Minimum Average Annual turnover criteria for the past 3 financial years (2023-24, 2022- 23 and 2021-22) for the bidder should be 120 Crore. b. The bidder should have positive operating profit during the last three financial years (2023-24, 2022-23 and 2021-22). c. Further, Net worth of the Bidder should be positive as on the end of the 31 March 2024.	Financials a. Minimum Average Annual turnover criteria for the past 3 financial years (2023-24, 2022-23 and 2021-22) for the bidder should be 120 Crore. b. The bidder should have positive operating profit during the last three financial years (2023-24, 2022-23 and 2021-22). c. Further, Net worth of the Bidder should be positive as on the end of the 31 March 2024. or In case the bidder entity is the result of a merger or acquisition or demerger or hive off, due consideration shall be given to the financial results of the merging entity or demerged entity as the case may be for the purpose of determining the minimum annual turnover. Thus, the financial documentation of the for the	No Change

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
					purpose of meeting the eligibility criteria should the bidder be in operation for a period of less than 2 financial years	

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
634	Minimum Eligibility Criteria	3	9	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/ any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH certified. Note: (i) Resources for CEHMax 10 resources shall be considered. The certification date must be prior to the date of publication of this RFP. (ii) If a resource is carrying more	The Bidder shall have minimum 100 security professionals supporting security and SOC solutions in India on bidder's payroll in/any of the following areas: - (a) Network Security (b) Data Security (c) Application Security (d) Cloud security (e) Security governance & incident management (f) Endpoint security (i) Vulnerability Management Of the above-mentioned professionals, atleast 50 professionals should be CISSP/ GCFA/ GCIH/GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CEH/ Comptia Security + certified. Note: (i) Resources for CEHMax 15 resources shall be considered. The certification date must be prior to the date of publication	Kindly refer to corrigendum

Sr. No.	RFP Reference File Name	Page	Clause	Existing Clause	Bidder's Queries / Comments / Suggestions / Deviations	Response
				than one certification, it shall be considered as one.	of this RFP. (ii) If a resource is carrying more than one certification, it shall be considered as one.	

Revised BOM and Commercials sheet

Sl. No.	Description	Total Quantity (For DC, DR and Near Site)	Quantity type	Price per unit per month in Rs.	GST in Rs.	Price per month including GST	Total Amount (Per Annum) including GST
1	SIEM as a service (With Incident Analysis, response and management services and Threat Hunting Services)	10000	EPS			0	0
2	SOAR as a service (with TIP)	5	Users			0	0
3	WAF as a service	300	mbps			0	0
4	DAM as a service	80	Databases			0	0
5	Web Proxy as a service	500	Endpoints			0	0

6	PAM as a service	500	servers			0	0
		200	privileged users			0	
7	EDR as a service	500	Endpoints			0	0
8	EASM as a service	40	Domains			0	0
9	SCM as a service	600	Assets			0	0
10	NBAD as a service	5000	FPS/PPS*			0	0
11	Any other cost (Breakup and description to be provided)						0
12	Grand Total (Per Annum) (1+2+3+4+5+6+7+8+9+10+11)						0
13	Grand Total (For 5 years)						0

Table 1: Minimum Commitment

Note:

1. Payment of the fixed resources as mentioned above (which is minimum commitment) shall be made on the basis of provisioning.

2. If the above-mentioned resources are not fully utilized (keeping the SLAs intact), NABARD reserves the right to use the tools within the minimum commitment at no additional cost.

* For the proposed NBAD solution 5000 FPS is envisaged. The bidder proposing PPS methodology shall consider a ratio of 1:5 (FPS:PPS) as a benchmark for proposing the solution.

Rate Chart

Sl. No.	Description	Measurement Factor	Unit Price per month including GST
1	SIEM as a service	Per 500 EPS	The rate will be paid based on the pro-rata cost quoted in the Bill of Materials (BOM) and the commercial for minimum commitments. The pro-rata cost should be valid for the entire contract period.
2	SOAR as a service (with TIP)	Per User	
3	WAF as a service	Per 300 mbps	
4	DAM as a service	Per DB	
5	Web Proxy as a service	Per Endpoint	
6	PAM as a service	Per Server / User	
7	EDR as a service	Per Endpoint	
8	EASM as a service	Per Domain	
9	SCM as a service	Per Asset	
10	NBAD as a service	Per 500 FPS/PPS	

Note:

1. Over and above the minimum commitment as mentioned above in table 1, Payment shall be made based on actual usage and not on the provisioning basis.

2. NABARD may explore any additional services with the vendor which are not mentioned in the Rate Chart at mutually agreed price during the period of the contract.

Revised Responsibility Matrix

Below mentioned is an indicative RACI matrix for the project:-

Category	Services	MSP/CSP	Application Team	MSSP	NABARD
	Application License		√		
	Cloud Service License	√			
License	Database License		√		
	Backup Software License	√			
	OS License		√		
	Antivirus with IPS/IDS		√	√	
	Compute	√			
	Storage	√			
	RAM	√			
	Network	√			
	DDOS Protected BW	√			
	Internet Bandwidth	√			

	Replication Setup	√	√		
Infrastructure	**DR Drills**	√	√	√	√
	Infra Monitoring	√			√
	Backup Operations and Management	√	√		
	Storage Management	√			
	OS management & Sys Admin	√	√		
Managed Services	**DB break Fix**		√		
	DB Performance Optimization		√		
	Replication Management	√	√		
	DR Run Book	√	√		
	Middleware Management		√		
	Application L1, L2 Support		√		
	Application Installation		√		
Application Support	**EOD, BOD, Batch Jobs, Month End Jobs (Business Process Support)**		√		
	APM		√		

	Security Tools	√	√	√	
	Physical Data Center Security	√			
	Host Security (Both server and client)	√	√	√	
	Data Security	√	√	√	
Managed Security	**Network Security**	√	√	√	
	Application Security	√	√	√	
	Security Tools(in Scope tools) Configuration and Deployment			√	
	Compliance Reporting (e.g., ISO27001, DPDP Act, etc)	√	√	√	√
	Regulatory Compliance	√	√	√	√
	VA-PT recommendations	√	√	√	√
	Patching (AV, OS, DB, application, middleware, Infrastrutcure, anything related to application, Security Tools)	√	√	√	
	SIEM			√	
	SOAR			√	

	Threat Detection and Alerting (for in scope tools)		√	√	√
	Incident Triage and Analysis			√	
	Incident Response (Initial Response)	√	√	√	
	Incident Response (Containment, Eradication, Recovery)	√	√	√	
	Threat Intelligence Integration		√	√	
	Security Reporting and Dashboards			√	
	Security Awareness Training (Reporting/Statistics)			√	
	Security Policy Updates and Maintenance (Tool specific policies)			√	
	Regular SOC Service and other security tool Reviews			√	√
	Change Management (related to security tools)		√	√	

	Security Tools Health Monitoring		√	√	
	Annual Health Checkup (Secuity Tools)			√	
	DAM Database activity monitoring		√	√	√
	PIM	√	√	√	
	SSL VPN	√	√		
	Anti DDoS	√	√		
	DLP		√		
	Performance Tuning	√	√	√	

NABARD shall be monitoring adherence to RACI matrix for all the stakeholders.