GUJARAT INFORMATICS LIMITED
Block No. 2, 2ND Floor, C & D Wing, Karmyogi Bhavan, Sector -10A, GANDHINAGAR - 382010

Corrigendum-1 dated 21-01-2026

Request for Proposal (RFP) for Selection of Implementing Agency for Providing External Attack Surface Management (EASM), Incident Response (IR) Services and End Point Management Solution for Gujarat Security Operations Center Department of Science & Technology, Government of Gujarat

(RFP # GIL/e-Gov/EASM/2025)
GeM Bid No: - GEM/2025/B/7052518

Please find the pre-BID queries responses & Annexure-1 & Annexure-2

(All bidders are advised to carefully read and consider all Pre-Bid Queries and Responses, with specific reference to Query Nos. 4, 26, 72, 76, 112, and 117. Further, Annexure-I and Annexure-II attached herewith shall be read as amendments to the relevant clauses of the RFP.)

For more details, visit www.gil.gujarat.gov.in & www.gem.gov.in

Pre-Bid Queries of Request for Proposal (RFP) for Selection of Implementing Agency for Providing External Attack Surface Management (EASM), Incident Response (IR) Services and End Point Management Solution for Gujarat Security Operations Center Department of Science & Technology, Government of Gujarat (GeM/Bid Number: GEM/2025/B/7052518 Dated: 01-01-2026)

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
1	Section 1.1 – Legal Entity	5 years operation mandatory	Request relaxation to 3 years for niche cybersecurity firms with Govt SOC experience.	As per RFP
2	Section 1.1 – Turnover	INR 16 Cr avg turnover	Request relaxation of turnover criteria to INR 8–10 Cr OR allow OEM-backed bidders.	As per RFP
3	Section 1.1 – Turnover	Pure financial threshold	Can technical score be given higher weightage than turnover?	As per RFP
4	Section 1.1 – Experience	Single ₹6 Cr order	Can cumulative multi-order experience be considered?	Revised Sr No.3 Section 1.1 as "The bidder must have successfully executed/completed at least 1) One single order of Rs. 5 Crores or 2) Two Orders each of Rs. 3 Crores or 3) Three Orders each of Rs.2 Crores for similar product / services in last 3 years to any central/ state Government / PSU/ Listed Company/BFSI. The project should include at least one activity comprising a scope of work similar to that defined in this RFP, such as: 1) External Attack Surface Management (EASM) services 2) End Point Management Solution Services Note :-The cumulative value of assignments repeatedly issued under an already awarded work order may be considered for meeting the prescribed work order value requirement.
5	Section 1.1 – Consortium	Consortium not allowed	Clarify if OEM + MSP prime bidder model is acceptable.	As per RFP
6	2.1.1 Asset Discovery	Internal + external assets	Is agentless discovery acceptable for internal assets?	Yes
7	2.1.1 Asset Discovery	Continuous monitoring	Expected frequency for full scans?	As per Section 3.1.1
8	2.1.2 Vulnerability	On-demand scans	Any limit on on-demand scans per month?	No
9	2.1.7 DRM	20 takedowns/year	Can unused takedowns be carried forward?	Yes
10	2.1.9 User Access	10 users	Named or concurrent licenses?	Both
11	2.1.10 Integration	SIEM/SOAR	Please confirm existing SIEM tools at GSOC.	Detail will shared after award of contract
12	2.1.14 Compliance	Multiple frameworks	Is mapping to NCRF mandatory from Day 1?	As and when required
13	2.2 IR Activation	On-demand IR	Expected average IR incidents per month?	Detail will shared after award of contract
14	2.2.2 IRRA	Readiness assessment	Is IRRA department-wide or sample-based?	Priority for CII, used department-wide when required
15	IR SLA	Onsite in 12 hrs	Are travel delays excluded from SLA?	As per RFP
16	IR Deliverables	Final report in 10 days	Can timeline vary based on incident complexity?	As per RFP
17	IR Hours	100 hours included	Can unused hours be rolled into proactive assessments?	As per section 3.2.11
18	2.3.2 Coverage	2000 endpoints	Does this include DR, test, staging?	yes
19	2.3.3 Infrastructure	Bidder to provide servers	Minimum hardware specs expected?	Require as per cover Scope of Work and SLA
20	Patch Mgmt	No reboot patches	Kernel patches reboot exemption?	Exempted in certain case after prior approval
21	Remote Control	Enabled	Is user consent mandatory?	As and when required
22	SBOM/QBOM	Mandatory	Accepted formats for submission?	Accepted in Standard format
23	SLA Penalty	Up to 10%	Is penalty service-wise or cumulative?	Separate invoices shall be raised for each of the three components of the RFP, and SLA penalties, up to a maximum of 10%, shall be levied independently for each respective component in accordance with the applicable SLA provisions.
24	Payment Terms	Quarterly	Can first payment be post go-live milestone-based?	As per RFP
25	Rate Applicability	Same rates for GoG	Is applicability mandatory for full contract term?	As per RFP
26	PBG	3% of TCV	Can PBG be phased or reduced post Year-1?	The Bidder shall submit a Performance Bank Guarantee (PBG) equivalent to five percent (5%) of the Contract Value of the EASM and EPM components, in accordance with the prevailing terms and conditions stipulated in the RFP
27	Contract Extension	Same cost	Will extension be mutually negotiated?	As per RFP
28	Section 1.1 – Experience	Single ₹6 Cr order	The number of such projects executed was limited, and the individual project values were comparatively small. Therefore, we request the authority to kindly consider the cumulative project value of ₹6 crore achieved through multiple orders while evaluating our experience.	As per response in Query#4
29	Section 1.1 – Consortium	Consortium not allowed	In view of the project scope and its technical complexity, we request the authority to kindly permit participation in this bid through a consortium.	As per RFP
30	2.1.1 Asset Discovery	Internal + external assets	Is agentless discovery acceptable for internal assets?	As per Query response#6
31	2.1.1 Asset Discovery	Continuous monitoring	Kindly clarify the expected frequency for full scans?	As per Query response#7
32	2.1.2 Vulnerability	On-demand scans	Any limit on on-demand scans per month?	No limit
33	2.1.7 DRM	20 takedowns/year	Can unused takedowns be carried forward?	Yes
34	2.1.9 User Access	10 users	Named or concurrent licenses?	Both
35	2.1.10 Integration	SIEM/SOAR	We request authority to kindly confirm existing SIEM tools at GSOC.	Detail will shared after award of contract
36	2.1.14 Compliance	Multiple frameworks	Is mapping to NCRF mandatory from Day 1?	As and when required
37	2.2 IR Activation	On-demand IR	Expected average IR incidents per month?	Detail will shared after award of contract
38	2.2.2 IRRA	Readiness assessment	Is IRRA department-wide or sample-based?	Priority for CII, used department-wide when required
39	IR Deliverables	Final report in 10 days	We request authority to kindly define timeline based on incident complexity and it may very based on complexity?	as per given in 3.2.9 in RFP
40	IR Hours	100 hours included	Can unused hours be rolled into proactive assessments?	Unutilised IR hours shall carry forward to subsequent years
41	2.3.2 Coverage	2000 endpoints	Does this include DR, test, staging?	Yes
42	SLA Penalty	Up to 10%	Is penalty service-wise or cumulative?	Query#23
43	Rate Applicability	Same rates for GoG	Is applicability mandatory for full contract term?	As per RFP
44	Bid Offer Validity GEM Doc/Page 1	180 Days	The bidder requests to reduce the bid validity to 90 days instead of 180 days, considering the current market volatility	As per RFP
45	3.1.4 Penalty RFP Doc/Page 27	SLA penalties up to 10% of quarterly invoice	Bidder Request to cap penalty @ 5% for the delayed/impacted time of delay instead of quarterly invoice value.	As per RFP

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
46	3.1.6.2 General Conditions RFP Doc/Page 28	3. The Service Provider must provide Performance Bank Guarantee (PBG) equivalent to 3% of total contract value valid for the entire contract period plus 60 days.	Bidder request to confirm on the PBG of 3%, which is contradicting with 5% PBG requirement under Section 4 GCC & GEM documents.	As per response in Query#26
47	3.1.6 Payment Terms of EASM RFP Doc/Page 28	Installation, configuration, and integration of EASM platform with GSOC (UAT sign-off) - 30% Go-Live and start of continuous monitoring - 30%	Bidder request for below changed in payment term Installation, configuration, and integration of EASM platform with GSOC (UAT sign-off) - 60% Go-Live and start of continuous monitoring - 10% Managed services, monitoring, and reporting -30%	As per RFP
48		Phase 3 – Quarterly Operations Payment in 8 equal quarterly instalments	Bidder request to release the payment monthly in arrears	As per RFP
49	3.2.11 Penalty for SLA Non-Compliance RFP Doc/Page 31	Delay in onsite deployment 1% of monthly retainer fee per hour delay, max 15%	Bidder request to clarify SLA Penalty is capped @10% per 3.1.4 clause, whereas 3.2.11 clause is capped @ max 15%. This is contradicting, kindly confirm on penalty cap.	It is clarified that the SLA penalty shall be capped at ten percent (10%) of the contract value for the EASM component and fifteen percent (15%) of the contract value for the IR service
50	Earnest Money Deposited (EMD) Page 39	The EARNEST MONEY DEPOSIT shall be forfeited: *No exemption for submitting the EMD will be given to any agency.	Bidder Request to confirm on EMD exemption, this is contradicting with GEM document -The seller also exempted from EMD submission with respect to clause “Sellers will get exemption from furnishing Bid Security Sellers / Service Provider having annual turnover of INR 500 Crore or more, at least in one of the past three completed financial year(s)”.	EMD exemption is applicable as per GeM GTC
51	Performance Security/Performance Bank Guarantee Page 39	The Successful bidder has to submit Performance Bank Guarantee @ 5% of total order value within 15 days from the receipt of notification of award/Contract Signing for the duration of warranty/contract	Bidder Request for 3% PBG on yearly rolling basis till contract + claim period	As per response in Query#26
52	New clause	Limitation of Liability	We request the inclusion of this clause- "Notwithstanding anything to the contrary contained herein or any other agreement between the parties, the total cumulative liability of the Bidder arising out of this Agreement and the subsequent Agreement executed between the parties shall not exceed in aggregate the amounts due and payable by GIL to the Bidder under the Agreement. This provision does not limit either party’s liability for: unauthorized use of intellectual property, death or bodily injury caused by their negligence; acts of fraud; nor any liability which may not be excluded or limited by applicable law However, Bidder shall not be liable to GIL for any special, indirect, incidental, consequential, exemplary, or punitive damages whether in contract, tort, or other theories of law, including loss of or damage to data, lost revenue or profits and downtime costs, even if such party has been advised of the possibility of such damages." Bidder requests inclusion of Limitation of liability clause as this clause will help mitigate risk of unlimited liability of HPE for contractual damages to a reasonable sum. Furthermore, GIL will still have the right to claim unlimited damages for instances of fraud, breach of law, IPR infirngement, death of personnel or damage to GIL's property. This makes the inclusion of this clause beneficial for both parties.	As per RFP
53	1.2.7.3	Earnest Money Deposit	Bidder requests clarification on whther EMD exemption is applicabel to this Bidder or if EMD shall be payable. In case it is payable, Bidder requests that forfeiture of EMD due to non-performance of contract signing as per clasue 1.2.7.3 e (ii) should be invoked only 90 days after the award of Bid to Bidder and with 30 days notice and cure period to cure such non-performance. Bidder requests that EMD shall not be forfeited for inability of the parties to reach a mutual agreement on the applicable terms and conditions. Bidder requests clarity that delays owing to ongoing negotiations on the finalization of terms and conditions of the Contract shall not be accounted towards the time period specified for the submission of the PBG/execution of the contract. Bidder requests that the forfeiture of EMD be invoked only where Bidder has been convicted for fraud. Additionally, Bidder requests that forfeiture of the EMD not be a cause for blacklisting / debarring unless it is owing to actions of a fraudulent nature.	As per RFP
54	1.2.7.5	Bid Validity	The bidder requests to reduce the bid validity to 90 days instead of 180 days, considering the current market volatility	As per RFP
55	2.1.13	Contract Period	TheBidder requests that any extension of contract term beyond two years should take place with mutual consent of both Parties.	As per RFP
56	Scetion 2	Scope of Work		Query is not mentioned
57	Section 3	Penalties		Query is not mentioned
58	3.2.11 Penalty for SLA Non-Compliance RFP Doc/Page 31	SLA Penalty	Bidder request to clarify SLA Penalty is capped @10% per 3.1.4 clause, whereas 3.2.11 clause is capped @ max 15%. Bidder requests overall cap of 5% of price payable for defective portion as the cap for SLA penalties.	As per query response #49
59	Section 4	Insection and Testing	Bidder requests that any inspection and testing should be conducted once annually with 10 days notice on matters pertaining only to Bidders performance, on business days with no unreasonable disruption to the Bidder's ordinary functioning. Bidder is not required to disclose any propreitary or cnfidential business information during such inspection that does not relate to its provision of services under this agreement. The inspection and testing if conducted by third parties on behalf of GIL, shall not be conducted by Bidder's competitors. Inspection shall not be given access to: 1.any information not related to the Services; 2.Bidder locations/premises (or portions thereof) that are not related to the Services; or 3.Bidder records or documents relating to the make up of Bidder’s internal overhead calculations or direct costs, their relationship to the service charges, any financial cost model, calculation of service charges or Bidder’s profitability; or 4. internal Bidder audit reports, or any summaries thereof.	As per RFP
60	Section 4	Performance Security	Bidder requests that Performance Security shall be forfeited only after failure of Bidder to cure any material breach where GIL shall provide a notice of breach to the Bidder and an opporutnity to cure the breach for 30 days after such notice; and such amount be limited to the actual losses suffered and subject to the Limitation of Liability.. The performance security shall be returned to the bidder on the last day of the validity of the agreement or on the last date of validity as per date of termination of contract, if the Agreement is terminated as per the provisions contained herein.	As per RFP
61	Section 4	Prices	Bidder requests that price variations owing to a change in taxes, quantity change and change in place of delivery should be permitted as these would be beyond the Bidder's control.	As per RFP

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
62	Section 4	Termination for Default	Bidder requests this clause to be amended so that termination for default shall be for material default only. Termination of Agreement shall take place only due to material failure of Bidder to deliver or perform obligations, material violations of terms and conditions and not for ordinary failure or ordinary breach. Termination for material breach shall only be invoked against Bidder in case Bidder ha failed to cure default or deliver services after GIL has provided notice of scuh default to Bidder and allowed a cure period of 30 days to Bidder after such default. Bidder suggests the following language for the same - "Either party may terminate this Agreement on written notice if the other fails to meet any material obligation and fails to remedy the breach within 30 days after being notified in writing of the details of the default." Bidder requests that the following statement should be deleted - d) If the Service Provider fails to conform to the quality requirement laid down/third party	As per RFP
63	Section 4	Termination for Convenience	Bidder requests this clause to be amended so that GIL provides a notice of 30 days before terminating for convenience and provides early termination fee if applicable and as mutually agreed between the parties.	As per RFP
64	Section 4		Bidder requests that the following provision be deleted as it may change the condition of the tender to cause unforeseen loss for the Bidder - GIL/ Gujarat Security Operation Center(GSOC), Gandhinagar, reserves the right: - To vary, modify, revise, amend or change any of the terms and conditions mentioned above	As per RFP
65	Section 4		Bidder requests that the following provision be deleted as it may change unforeseen loss of revenue and problems in revenue recognition for the Bidder - Gujarat Security Operation Center(GSOC) is free to phase out the work if it feels it necessary.	As per RFP
66	Section 4	Payment Terms	Bidder requests deletion of the following set-off clause as all penalties should be charged against the Bidder by raising a separate invoice - All payments will be subject to penalties for delays, as specified in the Service Level Agreement (SLA). In case of any penalties applied due to delays or non-compliance with SLAs, the corresponding deductions will be made before processing payments.	As per RFP
67	Section 4	Payment Terms	Bidder requests deletion of the follwoing penalty threshold as it is very onerous for the Bidder. "The overall penalty would be calculated cumulatively & it will be generally capped at 10% of QP amount. If the cap of overall penalty is reached in two consecutive Quarter, the penalty cap for the third Quarter onwards, for each Quarter will increase by 5% over the penalty cap for the preceding quarterly till it reaches 25% of the QP. In addition to the applicable penalty and the provisions pertaining to closure/termination of contract, the TENDERER shall be within its rights to undertake termination of contract if or anytime the penalty increases by 15% of the QP. Once the penalty cap has increased beyond 10%, if the bidder through better performance delivery for any Quarter, brings the leviable penalty below 10% then the computation of the 1st of the 2 consecutive Quarter as referred above will reset and will begin afresh."	As per RFP
68	Section 4	Payment Terms	Bidder requests that all invoices raised by the bidder be paid on a monthly basis within 30 days from the date of the invoice and all commercial off-the-shelf products and services accepted upon delivery and performance, and any objectively verifiable acceptance criteria only be applicable to deliverables arising out of service performance where the final contract will contain such provisions around a detailed acceptance procedure, including instances of deemed acceptance, acceptance period and rectification of defects.	As per RFP
69	New Clause		Bidder requests that the following provision be added to the Agreement for the protection of both parties - "Information exchanged under this Agreement will be treated as confidential if identified as such at disclosure or if the circumstances of disclosure would reasonably indicate such treatment. Confidential information may only be used for the purpose of fulfilling obligations or exercising rights under this Agreement, and shared with employees, agents or contractors with a need to know such information to support that purpose."	As per RFP
70	Section 1, Table1.1	Eligibility criteria, Point 3... Bidder Past Experience of work execution:	Bidder request to change the clause to " The bidder must have successfully executed/completed at least two of the 3 required solutions asked in the RFP viz EASM.Solution Incident response,End point Management	As per response in query#4
71	2.1 / page 15	Scope of work for External Attack Surface Management (EASM) Services	Request you to please let us know the count of primary domains to be covered as part of EASM and DRM	Primary domains are minimum 10 and aub-domains are Minimum 800 covered as a part of Scope
72	2.1 / page 15	Scope of work for External Attack Surface Management (EASM) Services	Request you to please let us know the count of GIL official social media handles and mobile applications to be covered as part of EASM and DRM.	It is amended in RFP that the "Social Media" component is removed from the Scope of Work. All other terms and conditions shall remain as per the RFP.
73	2.1.1 / page 15	Internal: Servers, endpoints, databases, IoT devices, network appliances.	Is this internet facing asset (external internet facing devices) ? As the requested service is - External Attack Surface Management (EASM), and Digital Risk Monitoring (DRM) in which external assets will be covered	Yes
74	2.1.7 / page 16	DRM should align with MeitY's Digital Risk Protection Guidelines.	We did not find the ' Digital Risk Protection Guidelines' in MeitY's website https://www.meity.gov.in/documents/guidelines?page=1 Request you to please share the Digital Risk Protection Guidelines.	Remove this clause from RFP
75	2.1.7 / page 16	Digital Risk Monitoring (DRM) Support takedown of: o Fake domains, phishing content, rogue mobile apps (min. 20/year).	What would be the maximum number of takedown required ? (example - 500 / unlimited)	As per RFP
76	2.1.8 / page 17	Reporting & Compliance Compliance mapping (ISO 27001, NIST, CERT-In, DPDPA, GIGW, NCRF).	Can you please elaborate more on this requirement. What kind of compliance your are looking at ? What has to be compliant ? The EASM solution or the report finding ?	It is amended that compliance with DPDPA and GIGW is removed from the Scope of Work. All other terms and conditions shall remain as per the RFP.
77	2.1.2 / page 15	Perform attacker simulation using OSINT	Can you please elaborate if we can perform active attacking on the vulnerable websites?	Simulated/Controlled environment/ on Stagging/UAT Platform
78	2.1.5 / page 16	Remediation Management & Workflow Integration	Can Integration to GSOC , EMS, SIEM/SOAR solutions can be done through Rest API?	As per RFP
79	2.1.9 / page 17	Platform features & user Access	Is SSO integration mandatory, or can we consider the approach using OTP-based MFA?	Expected solution with MFA and in case multiple solution from OEM,SSO is desirable.
80	2.1.11 / page 17	Training & Documentation	Shall the training's need to be done in offline or can be done online?	In Both mode accepted.Initially offline training required to targeted users of GSOC & GSDC as per RFP.

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
81	3.1.3 / page 27	SERVICE LEVELS AND UPTIME Phishing / Rogue App Takedown 24 hours	Different hosting provider / abuse report review committees / registrars have their own SLA / working geographic times to review and respond to any takedown request, which no other part have control over takedown request processing time. It might be difficult to commit any SLA related to takedown. Can the bidder get some relaxation with respect to takedown SLAs ?	“As per the RFP, however, in the event of third-party involvement or any unforeseen and uncontrollable situation, the Purchaser reserves the right to grant relaxation based on proper and verifiable evidence.”
82	3.1.4 / page 27	Penalty SLA penalties up to 10% of quarterly invoice 3 consecutive SLA failures . contract termination option	As SLA for takedowns are different for different hosting providers / registrars handling the request. Can the bidder get some relaxation with respect to SLA Penalty ? Can you please explain how the 3 consecutive SLA failures are counted with example.	As per response in Query#81
83	Compliance & Check list / page 60	Web/mobile app OWASP analysis	The OWASP analysis point was not present in the scope of EASM, request you to please elaborate on this requirement. Note - In passive assessment with no access to web and mobile applications, it may not be possible to cover OWASP top 10 threats for web and mobile.	Remove OWASP from this clause other terms as per RFP
84	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	How many documents like the cyber crisis management, SOPs, and departmental IR plans are currently in place?	Detail will shared after award of contract
85	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	How many departments/entities are currently within scope?	Primarily for state CII and further extended Department wide as and when required.
86	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	Does GoG prefer centralized workshops/awareness session or department-wise engagements?	No It is for GSDC, Phishing drill for DST can be arranged
87	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	How many office location are to be considered for the assessment?	Five
88	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	What security technologies are currently deployed (SIEM, EDR, SOAR, DLP, firewall etc.)?	Detail will shared after award of contract
89	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	Which is the current SIEM deployed?	Detail will shared after award of contract
90	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	What is the current EPS?	Detail will shared after award of contract
91	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	Is there an existing SOC, and what is its operating model (in-house, outsourced, hybrid)?	In house GSOC
92	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	Are cloud or third-party environments (SaaS, IaaS) included in scope?	Gujarat Governement has Privated Cloud in GSDC and all infrastructure deployed there are in Scope
93	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	Who are the expected participants for TTX (technical teams, leadership)?	DST Technical Staff and Officers
94	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	How many TTX's are expected in 1 year?	biannually
95	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	How many IR playbooks/runbooks currently exist?	Detail will shared after award of contract
96	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	Should playbooks be customized per department or standardized across GoG?	Bidder have to submit suggestions to Develop/Update IR Playbooks and Runbooks aligned with MITRE ATT&CK framework and GoG environment.
97	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	Is there a formally defined incident response team?	Detail will shared after award of contract
98	2.2.2 / page 19	Phase 1 – Incident Response Readiness Assessment (IRRA)	Does GoG already have a secure forensic lab or IR infrastructure?	No
99	2.3.2/ page 21	Coverage & Target Assets	What are the network devices in use with os.	Detail will shared after award of contract
100	2.3.5/ page 22	Agent & Architecture	What is the need of multitenancy please explain.	As per RFP
101	2.3.2/ page 21	Coverage & Target Assets	What type of the solution is required e.g. on-prem or SAAS	on-prem
102	7 / page 10	Consortium/ Subletting shall not be allowed	Can we include our third party partner to assist us in providing part of service ?	As per RFP
103	Section 1 Table 1.1 – Pre-Qualification Criteria, Sr. No. 2 (Financial – Turnover)	The bidder should have minimum annual average turnover of Rs. 16 Crores from IT/ITES services in the last three financial years (i.e. 2021-22, 2022-23 and 2023-24) as on 31st March 2024 for which bidder’s accounts have been audited.	Kindly clarify whether the turnover requirement of INR 16 Crores is mandatory, or whether a rationalised turnover (5-10 Cr.) may be considered based on the scope of work, as high turnover thresholds may restrict participation of technically capable bidders for specialised cybersecurity services.	As per RFP
104	Section 1 Table 1.1 – Pre-Qualification Criteria, Sr. No. 3 (Past Experience)	The bidder must have successfully executed/completed at least 1) One single order 2) Two Orders each of Rs. 4 Crores or 3) Three Orders each of Rs. 3 Crores for similar product / services in last 3 years to any central/ The project should cover similar activities and scope of work as defined in this RFP such as · External Attack Surface Management (EASM) services · Solution Incident Response (IR) Services · End Point Management Solution Services	Kindly clarify whether cumulative experience from multiple similar projects of lower individual value may be considered, as such cybersecurity services are typically executed through multiple modular engagements rather than single large-value orders.	As per response in Query #4
105	Section 1 - Technical Criteria, Sr. No. 2	The bidder should have a minimum of 5 qualified cybersecurity professionals on permanent payroll holding certifications such as CISA / CISSP / CEH / CCSP / CISM / OSCP / CRTP / CREST issued by globally recognized bodies like ISACA / (ISC)² / EC-Council / Offensive Security / CREST.	Kindly clarify whether certified professionals engaged on a contractual or project basis, along with permanent employees, may be considered, as cybersecurity resources are commonly deployed on a need-basis depending on project scope and duration.	As per RFP
106	Section 2.1.4 – Compliance & Governance	Must comply with: o CERT-In Guidelines (Current & later updates) · MeitY Localization Norms for Cybersecurity · NCIIPC's National Critical Information Infrastructure · DPDPA 2023,	Kindly clarify whether the EASM solution is required to be DPDP compliant itself, or whether it is expected to support the organisation in achieving DPDP compliance and produce everything on a single dashboard, as this distinction impacts solution design and scope alignment.	As per response in Query#76

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
107	Table 1.1: Pre-qualification Criteria Page: 10	The bidder must have successfully executed/completed at least 1) One single order of Rs. 6 Crores or 2) Two Orders each of Rs. 4 Crores or 3) Three Orders each of Rs. 3 Crores for similar product / services in last 3 years to any central/ state Government / PSU/ Listed Company/BFSI. The project should cover similar activities and scope of work as defined in this RFP such as · External Attack Surface Management (EASM) services · Solution Incident Response (IR) Services · End Point Management Solution Services	As we are MSME, can we get some relaxation on this requirement?	As per RFP
108	1.2.7.3 Earnest Money Deposit page 13	Earnest Money Deposit Rs. 16,00,000/- (Sixteen Lacs Only) in the form of Demand Draft an unconditional Bank Guarantee (which should be valid for 9 months from the last date of bid submission) of any Nationalized Bank/ Scheduled Commercial Bank (operating in India having branch at Ahmedabad/ Gandhinagar) in the name of "Gujarat Informatics Limited" payable at Gandhinagar (as per prescribed format given at Form-2) and it must be submitted along with the covering letter. Also, the bidder must submit the PoA (Power of Attorney) in physically form to the GIL before the due time of bid opening. Bidders can upload the scan copy of EMD on the portal.	As we are MSME, can we get some relaxation on this requirement?	EMD exemption is applicable as per GeM GTC
109	section 2.1.1 – Comprehensive Asset Discovery & Inventory (EASM section)	Continuous, automated identification and monitoring of all digital assets, including: o External (Internet-facing): Public IPs, domains, subdomains, APIs, web apps, open ports, exposed services. o Internal: Servers, endpoints, databases, IoT devices, network appliances. o Cloud Infrastructure: SaaS, IaaS, PaaS, storage buckets, server less functions across major cloud platforms. o Third-Party Assets: Vendor portals, partner systems, exposed code repositories.	For Section 2.1.1 on continuous discovery of external assets, could you please provide the expected asset count? This will help us plan the EASM coverage accordingly.	As per response in query#18 and 71 and other 200 Network devises,2 No of IPV4,2 No of IPV6 and please note may be vary based on future requirement.
110	2.1.11 Training & Documentation	2.1.11 Training & Documentation □ Training for GSOC cyber security team: minimum 2 sessions/year. □ SOPs, deployment run books, API documentation. □ Final handover report with implementation summary and roadmap.	Kindly confirm the maximum scope of training expected, including number of participants, duration, and whether any additional trainings beyond GSOC are required.	The training shall be conducted for the Technical Staff and Officers of DST. For other users, phishing simulation exercises may be carried out."
111	**Page No 10:** Bidder Past Experience of work execution	The bidder must have successfully executed/completed at least 1) One single order of Rs. 6 Crores or 2) Two Orders each of Rs. 4 Crores or 3) Three Orders each of Rs. 3 Crores for similar product / services in last 3 years to any central/ state Government / PSU/ Listed Company/BFSI. The project should cover similar activities and scope of work as defined in this RFP such as • External Attack Surface Management (EASM) services • Solution Incident Response (IR) Services • End Point Management Solution Services	The bidder must have successfully executed/completed at least 1) One single order of Rs. 6 Crores or 2) Two Orders each of Rs. 4 Crores or 3) Three Orders each of Rs. 3 Crores for similar product / services in last 3 years to any central/ state Government / PSU/ Listed Company/BFSI. The project should cover similar activities and scope of work as defined in this RFP such as • External Attack Surface Management (EASM) services ***OR*** **DNS Security** ***OR*** **DDos Protection** ***OR*** **DLP Solution** • Solution Incident Response (IR) Services ***OR*** **SIEM** ***OR*** **Database Access Monitoring** • End Point Management Solution Services	As per response in Query#4
112	**Page No 11:** Technical Criteria	The bidder should have at least 2 years of experience in providing External Attack Surface Management (EASM) and Digital Risk Monitoring / Digital Risk Protection (DRM/DRP) services/ End Point Management (EPM) Solution/ Incident Response (IR) Services in Government / PSU / Financial Institution / Large Enterprise organizations/Listed Companies in India during the last three (3) years (as on RFP release date	The bidder should have at least 2 years of experience in providing External Attack Surface Management (EASM) **OR DNS Security OR DDos Protection OR DLP Solution** and Digital Risk Monitoring / Digital Risk Protection (DRM/DRP) services/ End Point Management (EPM) Solution/ Incident Response (IR) Services **OR SIEM OR Database Access Monitoring** in Government / PSU / Financial Institution / Large Enterprise organizations/Listed Companies in India during the last three (3) years (as on RFP release date	The existing Technical Criteria table provided on Page No. 11 is hereby omitted and replaced with a new table included in Annexure-2 under Section 3.1.6.5 titled "Technical Criteria for EASM"

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
113	Page 10. Point 3 of Pre-qualification Criteria	The bidder must have successfully executed/completed at least 1) One single order of Rs. 6 Crores or 2) Two Orders each of Rs. 4 Crores or 3) Three Orders each of Rs. 3 Crores for similar product / services in last 3 years to any central/ state Government / PSU/ Listed Company/BFSI. The project should cover similar activities and scope of work as defined in this RFP such as ⍰ External Attack Surface Management (EASM) services ⍰ Solution Incident Response (IR) Services ⍰ End Point Management Solution Services	Request to relax this clause as below. The bidder must have successfully executed/completed at least 1) One single order of Rs. 6 Crores or 2) Two Orders each of Rs. 4 Crores or 3) Three Orders each of Rs. 3 Crores for similar product / services in **last 5 years** to any central/ state Government / PSU/ Listed Company/BFSI. The project should cover similar activities and scope of work as defined in this RFP such as ⍰ External Attack Surface Management (EASM) services/**Dark web monitoring** **OR** ⍰ Solution Incident Response (IR) Services **OR** ⍰ End Point Management Solution Services**/Enpoint and Server Protection**	As per response in Query#4
114	Page 11. Point 1 of Technical Criteria	The bidder should have at least 2 years of experience in providing External Attack Surface Management (EASM) and Digital Risk Monitoring / Digital Risk Protection (DRM/DRP) services/ End Point Management (EPM) Solution/ Incident Response (IR) Services in Government / PSU / Financial Institution / Large Enterprise organizations/Listed Companies in India during the last three (3) years (as on RFP release date	Request to relax this clause as below. The bidder should have experience in providing External Attack Surface Management (EASM)**/**Digital Risk Monitoring / Digital Risk Protection (DRM/DRP) services/ End Point Management (EPM) Solution/**Endpoint Protection/** Incident Response (IR) Services in Government / PSU / Financial Institution / Large Enterprise organizations/Listed Companies in India during the last **Five (5)** years (as on RFP release date	As per response in Query#112
115	Page 8. Fact Sheet EMD Exemption	The seller also exempted from EMD submission with respect to clause "Sellers will get exemption from furnishing Bid Security Sellers / Service Provider having annual turnover of INR 500 Crore or more, at least in one of the past three completed financial year(s)".	As per latest GeM terms and conditions, EMD Exemption for Service Provider having annual turnover of more than INR 500 Crore is not applicable anymore. Kindly confirm	Yes
116	Page 28	Delay penalty: 1% per week up to 5% max, beyond which contract may be cancelled	Request to relax this clause as below. Delay penalty: 0.5% per week up to 5% max, beyond which contract may be cancelled	As per RFP
117	Page 28 Payment Terms of EASM	Phase 1 – Implementation - 30% Post successful deployment, training to GSOC staff, and UAT sign-off Phase 2 – Operationalization- 30% On Successful Go-Live after FAT signoff Phase 3 – Quarterly Operations- 40% Payment in 8 equal quarterly instalments upon submission of SLA-compliant performance report, invoice, and GSOC approval	Request to amend payment terms as below to maintain financial viability of project. Licenses: 80% of License cost on delivery of licenses 20% on implementation Implementation: 70% on Implementation 30% after Go-live signoff Managed services: Quarterly advance	As per RFP
118	Page 28 Payment Terms	-	Kindly clarify payment terms for EPM Solution	As per Annexure-1 added in corrigendum
119	15 , 2.1	This RFP invites proposals from experienced and qualified vendors for provisioning of a comprehensive EASM solution encompassing External Attack Surface Management (EASM), and Digital Risk Monitoring (DRM) aligned	Kindly confirm if DRM Solution is also needed if yes what will be contract term. As EASM and DRM are two different solution	As per RFP
120	15 , 2.1.1	Continuous, automated identification and monitoring of all digital assets, including External (Internet-facing): Public IPs, domains, subdomains, APIs, web apps, open ports, exposed services. o Internal: Servers, endpoints, databases, IoT devices, network appliances. o Cloud Infrastructure: SaaS, IaaS, PaaS, storage buckets, server less functions [illegible]	Please share the detailed list of existing solutions along with their respective OEMs that need to be integrated with the solution."	As per response in Query#109 and more details may be shared after award of contract
121	21 , 2.3.3	Design, install, configure, and commission the latest EPM solution across desktops, servers, and workstations. Installation, configuration, and commissioning shall be carried out by the OEM or OEM-authorized	Please confirm number of users their location and types of assests	Detail will shared after award of contract
122	21 , 2.3.3	The EPM solution must provide full lifecycle management of Local site and DR sites assets, including patching, configuration, inventory, and security enforcement. DR endpoints must be manageable via multi-zone architecture, with offline policy enforcement, secure	Please specify DC and DR Locations	DC at Gandhinagar and Far DR at Faridabad and Near DR at Ahmedabad
123	22 , 2.3.3	Provide minimum 7-day onsite training.	Kindly confirm numbers of persons to be trained	All GSOC & GSDC officials and current GSOC O&M Team
124	-	General queries	Kindly confirm Project Execution Timelines for EPM Solution	As per Section 3.3 SLA & Other terms for EPM
125	3.2.11 Penalty for SLA Non-Compliance Page # 31	The RFP specifies a minimum of 100 IR hours annually (S. No. 11) and mentions that unutilized IR hours must be converted into training, proactive assessments, or professional certifications (S. No. 12). We seek clarification on the following	1) Billing Mechanism for Unutilized Hours: Will the OEM/SI be allowed to bill the minimum committed IR hours even if they remain unutilized during the contract period? If yes, should the billing be done at the same hourly rate as IR services or at a different rate for alternative services? 2) Conversion Process: Is there a defined ratio or conversion formula for converting IR hours into alternative services (e.g., 1 IR hour = 1 hour of training)? Should the OEM/SI propose this conversion ratio in the commercial bid? 3) Will GSOC provide prior approval for converting unutilized IR hours into alternative services? Is there a cap or limit on the number of hours that can be converted?	Unutilised IR hours shall carry forward to subsequent years

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
126	3.2.11 Penalty for SLA Non-Compliance Page - 31	The RFP mentions alternative services such as training, proactive assessments, or professional certifications but does not specify the scope or effort required. Please clarify:	1) Training: -What type of training is expected (e.g., Incident Response, Threat Hunting, Forensics)? -Should training be onsite or remote, and what is the minimum duration per session? 2) Proactive Assessments: What specific assessments are expected (e.g., Purple Team exercises, Threat Simulation, Configuration Review)? Should these assessments include reporting and remediation recommendations? 3) Professional Certifications: Which certifications are acceptable ?	As per RFP
127	2.1.1 Comprehensive Asset Discovery & Inventory Pg.15	Continuous, automated identification and monitoring of all digital assets, including: o External (Internet-facing): Public IPs, domains, subdomains, APIs, web apps, open ports, exposed services. o Internal: Servers, endpoints, databases, IoT devices, network appliances. o Cloud Infrastructure: SaaS, IaaS, PaaS, storage buckets, server less functions	Request to provide the SaaS, IaaS, PaaS, storage buckets, server less functions across major cloud platforms inventory, also confirm if there is any SaaS application is being leveraged from outside India. Please confirm the list of IoT devices to be monitored	As per RFP
128	2.1.9 Platform Features & User Access Pg. 17	Deployment: Preferably SaaS; on-prem. or private cloud option if mandated.	please confirm if SaaS model on Public cloud is feasible.	Yes
129	M. Log, data forwarding and Integration Pg. 25	Log, data forwarding and Integration	request to confirm if bidder has to factor the log storage or Purchaser will provide the same and bidder has to forward the logs to the log store.	As per RFP and Bidder has to forward logs
130	2.1.1 Comprehensive Asset Discovery & Inventory Pg.15	Continuous, automated identification and monitoring of all digital assets, including: o External (Internet-facing): Public IPs, domains, subdomains, APIs, web apps, open ports, exposed services. o Internal: Servers, endpoints, databases, IoT devices, network appliances. o Cloud Infrastructure: SaaS, IaaS, PaaS, storage buckets, server less functions across major cloud platforms. o Third-Party Assets: Vendor portals, partner systems, exposed code repositories.	1)Internal asset discovery will not be possible for EASM tool, as it will scan only external facing assets of organization, request you to please remove the internal scope from EASM.	May be consider
131	2.1.4 Risk Prioritization & Scoring Pg.16	☐ Risk scoring to factor in: o Business impact, exploitability, exposure duration, regulatory risk. ☐ Support for custom risk models based on GSOC's internal framework. ☐ Visualization of risk posture and trend analysis dashboards.	Need more clarity, as EASM has its own Risk Model, no customization is allowed on risk models.	As per RFP
132	2.1.5 Remediation Management & Workflow Integration Pg.16	Provide contextual, actionable remediation steps. ☐ Validate remediation post-fix with closed-loop verification. ☐ Provide all data, logs, alerts, incidents etc. for Integration with: o GSOC (Audit, Assets, Advisory modules) o EMS, NMS, SIEM/SOAR, DevSecOps CI/CD tools. ☐ SLA-driven remediation tracking and escalation workflows.	Need more clarity, As EASM provides exact steps to be taken to remediate any issues, SLA tracking and Escalations has to be managed with ticket platform like SNOW or SOAR with external integrations	As per RFP
133	2.1.6 Continuous Monitoring & Alerts Pg.16	☐ 24x7x365 monitoring of: o Configuration changes, asset exposure, emergent threats. Real-time alerts via: o Email, SMS, GSOC Dashboard. ☐ Baseline Deviation Detection: Notify deviations from secure-state baselines	Request you to make SMS as optional	As per RFP
134	2.1.7 Digital Risk Monitoring (DRM) Pg.16	☐ Monitor: o Dark web, paste in, underground forums, app stores. o Impersonation attacks, phishing sites, rogue applications. ☐ Generate alerts for: o Credential leaks, brand abuse, data exposure. ☐ Support takedown of: o Fake domains, phishing content, rogue mobile apps (min. 20/year). ☐ DRM should align with MeitY's Digital Risk Protection Guidelines.	Alerts for Credentials leak and data exposures are covered with TI & ASM, please remove it from DRM SOW	As per RFP
135	2.1.8 Reporting & Compliance Pg.17	☐ Daily, weekly, and monthly reporting dashboards. ☐ Executive summary reports with KPIs/KRIs. ☐ Compliance mapping (ISO 27001, NIST, CERT-In, DPDPA, GIGW, NCRF). ☐ Full audit logs and policy enforcement reports. ☐ Visibility dashboards for Department Heads and Nodal Officers	DRM generally doesn't have any compliance mapped to it; it works on brand abuse and trademark abuse cases. Please elaborate for our understanding.	need to follow international standard / framework for report prepareation

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
136	2.1.12 Deliverables Pg.17	1. Fully functional EASM platform with GSOC-integrated dashboard access. 2. Dynamic asset inventory and threat exposure visibility. 3. Monthly threat landscape and executive summaries. 4. Remediation status reports with SLA adherence. 5. Incident and risk trend dashboards (aligned with NCRF). 6. Takedown reports (for phishing/impersonation sites). 7. DPDPA & CERT-In aligned compliance documentation.	DRM generally doesn't have any compliance mapped to it; it works on brand abuse and trademark abuse cases. Please elaborate for our understanding.	need to follow international standard / framework for report prepareation
137	2.1.14 Compliance & Governance Pg.17	☐ Must comply with: o CERT-In Guidelines (Current & later updates) o MeitY Localization Norms for Cybersecurity Products o NCIIPC's National Critical Information Infrastructure Framework o DPDPA 2023, ISO 27001 ☐ Execution of SLA and NDA before onboarding. ☐ Adherence to GSOC's governance and audit guidelines.	DRM generally doesn't have any compliance mapped to it; it works on brand abuse and trademark abuse cases. Please elaborate for our understanding.	need to follow international standard / framework for report prepareation
138	3.2.11 Penalty for SLA Non-Compliance for IRR Pg.31-33	Compliance Table & SLA	IRR is a service hence to enable SI to participate, request you to add Bidder/OEM for all compliance and SLAs.	It is added Service provider/OEM for Compliance Table & SLA
139	3.1 SLA & Other terms for EASM Pg.26	Takedown Request Execution Within 72 hours of GSOC approval Report with evidence 2% penalty per delayed takedown & Social Media Abuse Removal	Any social Media Abuse cases would take at least 7 Days more or less, request you to change the SLA to 7 days	As per response in Query#72
140	3.1.3 SERVICE LEVELS AND UPTIME	SLA Description Requirement Minimum Service Uptime 99.90% Phishing / Rogue App Takedown 24 hours Browser Blocking (if takedown not possible) 48 hours Domain Take Down Time 72 hours Social Media Abuse Removal 48–72 hours TI Critical Alert Reporting 4–6 hours EASM Report 3–7 days	1)As per 3.1.1 Service Level Agreement (SLA), Platform Availability (Uptime)should be ≥ 99.5% monthly uptime, request you to please modify and share exact requirement. 2) Any social Media Abuse cases would take at least 7 Days more or less, request you to change the SLA to 7 days. 3) As Takedown involves multiple third parties involvement, SLA should be mutually decided on case to case basis considering availability of related trademarks/supporting documents	Response is respectively 1) EASM and DRM reporting monitoring Platform must be available all time 2) social Media is removed from Scope 3) As per RFP (If third parties involvement and other issues arise Purchaser have right for relaxation for such consideration based on proper evidence)
141	2.3.5 Technical Features A. Agent and Architecture Pg.22	Agent software must be deployed on all managed Endpoints. Support Windows, Ubuntu, RedHat, CentOS, Rocky Linux in physical, virtualized, containerized form. Must operate without AD/domain dependency but support AD integration.	Kindly clarify the intent of the term "containerized form" in the above clause. In most enterprise endpoint management models, containers are ephemeral workloads and do not typically support a persistent endpoint agent installation inside the container (unlike physical/virtual machines and host OS). Request to Rephrase as "Agent software must be deployed on all managed endpoints/servers running Windows, Ubuntu, RedHat, CentOS, Rocky Linux in physical and virtualized environments".	As per RFP
142	2.3.5 Technical Features B. Patch Management Pg.22	Provide patching of OS, Application, Database, Middleware, Virtualization platforms, Security Tools, Packages	Kindly clarify the detailed scope for patching under the above clause. Request you to provide the list of products/technologies and versions expected to be covered for patching (Applications, Database, middleware, Virtualization platforms, Security tools and packages).	As per RFP
143	2.3.5 Technical Features F. Remote Control Pg.24	Role-based restrictions for control, reboot, file transfer	Kindly clarify whether the intent of the above clause is to ensure role-based access control (RBAC) for remote actions such as remote control and reboot, and whether file transfer is mandatory as part of remote control for all use cases. In many regulated environments, file transfer over remote sessions is treated as a separate security-sensitive feature and may be governed by organization policy. Requesting to amend as following "Role-based restrictions for control and reboot.	As per RFP
144	2.3.5 Technical Features M. Log, data forwarding and Integration Pg.25	Behavioural analytics, IOC scanning, threat hunting	Request you to confirm whether IOC scanning and threat hunting are mandatory capabilities within the endpoint management platform itself, or if these functions can be delivered through an integrated SOC/EDR/SIEM stack (as separate components/tools) while the endpoint management solution provides device control, hardening, and operational management. Since threat hunting and deep IOC scanning are typically aligned to EDR/XDR/SIEM platforms and SOC operations, kindly consider revising the clause to avoid ambiguity, as below: "Behavioural analytics for endpoint activity (as applicable).	As per RFP
145	2.3.5 Technical Features N. SBOM, QBOM Preparation & Supply Chain Risk Pg.25	Should provide SBOM, QBOM generation natively / third-party SBOM, QBOM without additional agent	As part of SBOM we will fetch below attributes for software components, - component name - component version - vendor - mapped software - filename - license - location - checksum - purl - description - vulnerability count - release date - dependencies	As per Cert-in guideline
146	General	Number of Top Level Domains and total subdomains to be considered.		As per response in Query#71
147	General	Any other integration required other than SIEM within GSOC, please suggest		As per RFP
148	General	Name of the Cloud Vendor (AWS/Azure/GCP) if any		Detail will shared after award of contract

Sr No	RFP reference	Content/Clause of RFP requiring Clarification	Clarification Sought/Suggestion	Tentative Response
149	General	For EPM post installation, patching is continuous process, is there additional manpower required to oversee overall patching and onboarding of agents and other product technical issues.		No additional manpower required for said activity and Scope and SLA as per RFP
150	Eligibility and Evaluation Criteria; Table 1.1: Pre-qualification Criteria; 3. Bidder Past Experience of work execution: page-10	The bidder must have successfully executed/ completed at least 1) One single order of Rs. 6 Crores or 2) Two Orders each of Rs. 4 Crores or 3) Three Orders each of Rs. 3 Crores for similar product / services in last 3 years to any central/ state Government / PSU/ Listed Company/BFSI. The project should cover similar activities and scope of work as defined in this RFP such as External Attack Surface Management (EASM) services Solution Incident Response (IR) Services End Point Management Solution Services	In view of the niche technology nature of the project and to ensure wider, high-quality participation while maintaining due diligence, we propose the following clarifications/changes to the qualification criteria: 1. **Project Experience Evidence**: The Bidder/OEM may showcase relevant project experience to meet this criterion (including niche technology implementations of similar scope and complexity). 2. **Global Project References**: The Bidder/OEM may submit project references executed for Indian/global clients, provided the scope, scale, and technology stack are comparable to the present requirement. 3. **No of Orders/Project:** The bidder/OEM can showcase at the max 3 purchase order having cumulative value as per the criteria. 4. **Acceptable Proof of Execution/Status**: The Bidder/OEM may submit any of the following as documentary evidence: - Purchase Order/Work Order/MSA along with a Project Completion/Execution Certificate; **OR** - A Chartered Accountant (CA) Certificate specifying client name, project scope, key deliverables, contract value, start/end dates, and current status (ongoing/completed). These adjustments would help demonstrate genuine capability without diluting	As per response in Query#4
151	Eligibility and Evaluation Criteria; Table 1.1: Technical Criteria; 1. page-11	The bidder should have at least 2 years of experience in providing External Attack Surface Management (EASM) and Digital Risk Monitoring / Digital Risk Protection (DRM/DRP) services/ End Point Management (EPM) Solution/ Incident Response (IR) Services in Government / PSU / Financial Institution / Large Enterprise organizations/ Listed Companies in India during the last three (3) years (as on RFP release date	In view of the niche technology nature of the project and to ensure wider, high-quality participation while maintaining due diligence, we propose the following clarifications/changes to the qualification criteria: 1. **Project Experience Evidence**: The Bidder/OEM may showcase relevant project experience to meet this criterion (including niche technology implementations of similar scope and complexity). 2. **Global Project References**: The Bidder/OEM may submit project references executed for Indian/global clients, provided the scope, scale, and technology stack are comparable to the present requirement. 3. **No of Orders/Project**: The bidder/OEM can showcase at the max 3 purchase order having cumulative value as per the criteria. 4. **Acceptable Proof of Execution/Status**: The Bidder/OEM may submit any of the following as documentary evidence: - Purchase Order/Work Order/MSA along with a Project Completion/Execution	As per response in Query#112
152		a suitable clarification or corrigendum allowing Startup India–registered entities and MSMEs to avail exemptions as per extant government guidelines, while incorporating the above technical and compliance requirements to ensure effective project execution.	We write with reference to the Request for Proposal (RFP No. GIL/e-Gov/EASM/2025, GeM Bid No. GEM/2025/B/7052518) issued by Gujarat Informatics Limited (GIL) for the selection of an implementing agency to provide External Attack Surface Management (EASM), Incident Response (IR) Services, and an End Point Management (EPM) Solution for the Gujarat Security Operations Center. In this context, we respectfully request GIL to consider extending applicable exemptions and relaxations for Startups and Micro, Small, and Medium Enterprises (MSMEs), in alignment with the prevailing policies and guidelines of the Government of India. Relaxations related to Earnest Money Deposit (EMD), turnover thresholds, and prior experience criteria would encourage wider participation from technically capable startups and MSMEs. Concurrently, to ensure solution authenticity, accountability, operational resilience, and adherence to global cybersecurity best practices, we humbly propose that participating organizations meet certain technical, operational, and governance-related requirements, including: Availability of an in-house Digital Forensics and Incident Response (DFIR) team, with proven expertise in cyber investigations, evidence handling, and incident response. Compliance of the Security Operations Center (SOC) with the Digital Personal Data Protection (DPDP) Act, ensuring lawful processing, storage, protection, and breach management of personal data.	As per RFP
153	Pre qualification Criteria ,point no 3	The project should cover similar activities and scope of work as defined in this RFP such as External Attack Surface Management (EASM) services Solution Incident Response (IR)	This clause is resctictive and a CPSU like BSNL may not able to participate in this hence it is requested to include ongoing projects and similar projects having Network detection and response system work profiles	As per RFP
154	Pre qualification Criteria ,point no 7	Consortium/ Subletting shall not be allow	Looking at the size , wider and complex scope of the project it is requested to allow consortium/Subletting.	As per RFP

Annexure-1 (Payment Terms – EPM Solution)

1. **Payment Structure**
   The total contract value shall be divided into:

   - **One-time Implementation & Deployment Cost**, and
   - **Recurring Annual Subscription, Support & Maintenance Charges** for five (5) years.

2. **Implementation & Go-Live Payment(80% of Contract value of EPM Solution)**

   - **60%** of the one-time implementation cost shall be paid after successful installation, configuration, and submission of installation report.
   - **20%** shall be paid after **User Acceptance Testing (UAT)** and issuance of **Go-Live Certificate** by the Department/GIL.

3. **Annual Subscription & O&M Payments(20% of Contract value of EPM Solution)**
   The remaining amount towards EPM licenses, platform usage, on-prem hosting, monitoring, updates, and technical support shall be paid **annually in arrears** as follows:

Year	Payment Trigger	Percentage
Year-1	After 12 months of satisfactory service from Go-Live	4%
Year-2	After 24 months of satisfactory service	4%
Year-3	After 36 months of satisfactory service	4%
Year-4	After 48 months of satisfactory service	4%
Year-5	After 60 months of satisfactory service	4%

(Total recurring payments = 50% of contract value of EPM)

5. **No Advance Payment**
   No advance payment shall be made. The Department / GIL shall release all payments only after verification of deliverables and certification in quarterly/half annually/yearly basis.

6. **Statutory Deductions**
   Applicable deductions such as **TDS, GST-TDS, penalties, and liquidated damages** shall be made as per Government rules.

Note :- All other terms and conditions are applicable as per RFP

Annexure-2 Technical Criteria for EASM

Sr.	Requirement	Documentary Evidence Required
1	The bidder should have at least **2 years of experience** in providing **External Attack Surface Management (EASM)** and **Digital Risk Monitoring / Digital Risk Protection (DRM/DRP)** services in India.	Documentary Proof such as order implementation / contract execution copy / Work Order / Completion Certificate.
2	The bidder should have successfully implemented **EASM and DRM/DRP services** for a minimum of **two (2) Government / PSU / Financial Institution / Large Enterprise organizations in India** during the last **three (3) years** (as on RFP release date).	Documentary Proof such as implementation certificate / contract execution copy / Work Order / Performance Certificate.
3	The bidder should have a minimum of **5 qualified cybersecurity professionals** on permanent payroll holding certifications such as **CISA / CISSP / CEH / CCSP / CISM / OSCP / CRTP / CREST** issued by globally recognized bodies like **ISACA / (ISC)² / EC-Council / Offensive Security / CREST**.	Copy of valid certificates and an undertaking on company letterhead confirming employment status.
4	The bidder should have a **direct support presence in Gujarat** (Ahmedabad/Gandhinagar region). In case a direct office is not available, the bidder must provide an undertaking to ensure **24×7 onsite support within Gujarat and support availability at national level locations** whenever required by GSOC without additional cost.	Letter of undertaking / confirmation on company letterhead.