Sun Petrochemicals Private Limited
8th,9th & 10th Floor, ATL Corporate Park, Saki Vihar Road,
Powai, Mumbai - 400 072, Maharashtra, BHARAT.
CIN: U24219GJ1995PTC028519
Tel: +91 22 69325300, + 91 22 28470484
Website: www.sunpetro.com; Email Id: info.sunpetro@sunpetro.com

No. SunPetro/Bhaskar/Cyber Security/2025-26/SPPL-242/Bulletin-1 **Date: 12.11.2025**

BULLETIN #1

Sub: Supply & Installation of Cyber Security Operation Centre (SOC) at Bhaskar-I Field in Gujarat

Ref: Tender No. SunPetro/Bhaskar/ Cyber Security /2025-26/SPPL-242

Sun Petrochemicals Private Limited (**SunPetro)**, hereby authorized following amendment / clarification in the above referred RFQ/ Inquiry:

Sr No	Bidder Query	SunPetro Response
1	Kindly confirm whether the CERT-In empanelment requirement can be amended to allow fulfilment through a third-party CERT-In empaneled partner, with whom we have formal collaboration, while the overall SOC operations and delivery remain under vendor responsibility as the prime bidder.	No. Primary agency needs to be Cert-IN empaneled
2	Kindly amend the clause as: Minimum Qualification: Proven skills in OT Security (IEC 62443 or similar), Digital Forensics, and Incident Response and Virtual CISO (v-CISO) or CISO-as-a Service (CaaS) delivery. Simple Explanation: The bidder / OEM must understand both IT and industrial (OT) systems, how to protect them, investigate cyber incidents correctly, and provide ongoing strategic cybersecurity governance through a Virtual CISO model.	Explanation is proper
3	Request SunPetro to share a complete and finalized asset inventory covering IT, OT, Cloud, Network, Applications, Security devices and field locations. This will enable accurate onboarding, sizing, compliance and SLA adherence.	Asset inventory already part of tender doc Kindly Refer to the tender Document.
4	Confirm that any additional devices, users, applications, log sources or new sites onboarded post-award shall be treated as a Change Request (CR) with commercial implications agreed mutually.	Yes
5	The SOW contains open-ended terms like “including but not limited to”. Requesting replacing with a defined scope annexure to avoid interpretation issues and ensure bounded contractual obligations.	Currently scope will be in line with Bid documents. Any changes during detailed engineering will be addressed via change control
6	Requesting clarity that OEM coordination, patching, firmware upgrades and downtime approvals for OT/ICS/SCADA systems shall rest with SunPetro/OEMs. Bidder’s role will be advisory only, as these environments are OEM-controlled.	Yes. Advisory and Monitoring will be part of Bidder scope
7	Clarify that any travel for onsite support (plant/CPF/rig/field) will be on actuals including travel, stay and logistics, since SOC pricing assumes remote delivery.	Yes
8	Request clarity on ownership and cost responsibility for SIEM, SOAR, EDR/XDR, TI, UEBA, OT collectors, forensic tools and log storage infra (on-prem/cloud). Bidder assumes no tool/infra cost unless explicitly included in commercials.	SIEM + SOAR ownership with Bidder. Rest of tools with SunPetro

9	Confirm that log ingestion, storage, archival and retention infra (180 days – 1 year) will be provided and funded by SunPetro, unless priced in the financial bid. Retention infra has a significant cost impact.	Agree
10	Request confirmation that EPS/log volume/retention increases or new integrations beyond agreed baseline will be handled via a billable CR.	Agree
11	Confirm that Bidder shall not be held responsible for performance or availability issues of third-party/OEM products not under its administration.	Agree
12	If a specific OEM stack is mandated by SunPetro, Bidder's responsibility will be limited to service delivery, with OEM responsible for tool performance & feature limitations.	Agree
13	Request SunPetro to share the detailed SLA & penalty framework (MTTD/MTTR, reporting, availability, false positives etc.) for review before submission, to ensure alignment and accurate costing.	Bidder to share their proposed solution along with SLA matrix
14	Recommend capping overall penalties to a maximum of 5% of monthly billing to maintain commercial balance. Request confirmation.	Tender condition shall prevail
15	Confirm that SLAs will not apply where delays or impact are due to Force Majeure, OEM dependencies, customer delays, lack of access/approvals or environmental factors beyond Bidder control.	As per scope
16	Request confirmation that incidents caused by pre-existing vulnerabilities or legacy issues (identified during onboarding) will be excluded from penalties until remediation is completed.	Complete assessment & Remediation to be provided by Bidder
17	Request clarity that MTTD/MTTR timers start only after required access, credentials and approvals are provided. Delays should pause SLA timers.	Complete assessment & Remediation to be provided by Bidder against acceptance by SunPetro
18	Proposed that Bidder's liability is capped to 12 months of contract value or INR 50 Lakhs (whichever is lower), with standard carve-out for Gross Negligence/Willful Misconduct.	Tender condition shall prevail
19	Seek confirmation that Bidder will not be liable for consequential or business losses, including production downtime or reputational impact.	Tender condition shall prevail
20	Clause 3.28 mentions 5% PBG, whereas NIT mentions 10%. Request confirmation on the correct PBG % and validity period to factor into commercials.	Bidder to consider, 10% PBG of the total contract value
21	Clarify whether Digital Forensics (DFIR), evidence collection and chain of custody are part of base scope or to be charged separately. DFIR requires specialized skillsets and tools.	Charged separately.
22	Request clarity if IR includes hands-on remediation & recovery, or is limited to triage, containment and advisory. If full IR is expected, it should be separately priced due to onsite and OEM dependency effort.	IR included hand-on remediation & recovery. This will part of technical evaluation criteria
23	Recommend default read-only access for SOC team. Any privileged access to be provided only through written approval per activity.	Agree
24	Request definition of SLA for VPN/Firewall/Access provisioning (e.g., 48 hours). Any delays to be excluded from MTTR/MTTD calculations.	SLA will be defined once vendor is finalized. Agree
25	BOQ states contractors bear logistics cost. Request clarification if ad-hoc onsite support requested by SunPetro will be reimbursed, since remote model assumes no recurring onsite presence.	Please factor one dedicated resource on site
26	Request a 60–90-day transition and stabilization period, with no SLA penalties during this time as tuning & baselining is essential for SOC accuracy.	Green field project
27	Request nomination of a single SunPetro SPOC authorized for change approvals, incident decisions and communication to ensure faster response.	Part of Program Management

28	Confirm that DFIR, malware analysis and deep-dive IR beyond initial triage will be chargeable as per rate card or SOW.	Agree
29	Request clarity on number of IR cases included (if any) per year/quarter. Additional IR to be chargeable at agreed rates.	this is perpetual professional service
30	Request definition of # of proactive threat hunts per month included in scope; additional hunts to be chargeable.	This is perpetual professional/operational service as and when required
31	Confirm whether Red Teaming / Purple Teaming / breach simulation are included or will be offered as separate SOW-based engagements.	Separate
32	Clarify that Bidder's IR role is advisory unless expressly contracted for hands-on cleanup, remediation and rebuild, which would require separate pricing.	IR included hand-on remediation & recovery. This will part of technical evaluation criteria
33	Confirm that OT monitoring sensors, taps, SPAN ports, diodes/UDGs will be provided by SunPetro or added to BOQ.	Agree part of Sun Petro deliverables
34	Confirm that OEM coordination for OT systems (patches, upgrades, compatibility checks) will remain with SunPetro/OEMs.	yes
35	Request confirmation that Bidder will not be liable for OT outages or safety events, unless due to proven Gross Negligence.	Yes
36	Clarify if compliance audit execution and evidence collection (CERT-IN/DPDP/ISO) are advisory only or part of scope. If included request scope limits.	Advisory only
37	Request detailing of vCISO hours/month, key deliverables & overage rates for clarity and to avoid open-ended effort.	Bidder to propose as per their best-fit proposition with in-depth scope an services. This will be part of technical evaluation
38	Confirm that audit-driven enhancements requiring extra tools/resources will be handled through CR with cost impact mutually agreed.	Agree
39	Request that termination for convenience requires 90-day notice plus payment for committed but unutilized orders and transition support.	Tender condition shall prevail
40	Confirm that playbooks, detection rules, SOAR workflows and methodologies remain Bidder IP; SunPetro receives usage rights for contract duration.	Agree
41	Request 30–90 days of structured transition-out, with clarity on whether this is included or chargeable, and define expected handover deliverables.	Agree
42	Briefly describe your organization's core operations and IT/OT landscape.	Exploration & Production of Oil & Gas with multiple sites SCADA & DCS Setup
43	List primary & secondary data centers, cloud regions, and remote sites.	Primary DC at HO Mumbai & Secondary at Gujarat, total sites are 6 including HO Mumbai
44	Approx. number of servers, endpoints, and network devices?	32 Servers, 510 Endpoints, approx. 25

45	What are the primary drivers for MSOC setup (compliance, visibility, threat detection, etc.)?	Threat Detection & Visibility
46	☐ Centralized ☐ Distributed ☐ Virtual / Cloud SOC	Centralized
47	☐ In-house ☐ Co-managed ☐ Fully Managed ☐ Hybrid	Hybrid/Fully Managed
48	☐ 24x7 ☐ 8x5 ☐ On-call	24X7
49	What's your expected deployment timeline?	Two Months
50	How many sites, VLANs, and data centers exist?	Primary DC at HO Mumbai & Secondary at Gujarat, total sites are 6 including HO Mumbai
51	Which sources will feed the SOC (firewalls, IDS/IPS, endpoints, applications, cloud)?	FW, IDS/IPS, Endpoints & application
52	Preferred SIEM (Q Radar, Splunk, Azure Sentinel, ManageEngine, etc.)	Qradar, Splunk, Azure
53	Which cloud platforms are used (AWS, Azure, GCP, SaaS)?	Azure
54	Which EDR/XDR tools are deployed?	Trend Vision
55	Do you have an existing feed (MISP, Anomali, Recorded Future)?	NO
56	Case Management Tool: JIRA, ServiceNow, The Hive, or custom?	JIRA OR Custom
57	How many servers, endpoints, network devices, and cloud resources will be onboarded?	32 Servers, 510 Endpoints, approx. 25, Five Cloud Instance
58	Are OT environments included in SOC scope?	Yes
59	List critical applications (ERP, SAP, CRM, etc.)	SAP, SCADA
60	Which use cases are prioritized (malware, phishing, exfiltration, insider threat)?	Ransomware, Malware, Phishing
61	What's the required log retention period (30 / 90 / 180 / 365 days)?	180 days
62	Do you require proactive hunting, and how frequently?	Yes
63	Should SOC perform full IR or escalate to internal teams?	Full IR
64	Do you follow ISO 27001, NIST CSF, RBI Cybersecurity Framework, etc.?	ISO 27001, NIST CSF
65	What reports or dashboards are expected (PCI DSS, GDPR, DPDP)?	Industry best
66	Define metrics like MTTD, MTTR, alert volume, SLA adherence.	KPI & SLA to define
67	Daily, weekly, or monthly summaries?	Daily & Monthly
68	Will logs be collected via Syslog, API, agent, or VPN tunnel?	API Preferred
69	On-premises, cloud-hosted, or hybrid?	Hybrid/Fully Managed
70	Is a backup SOC or DR site needed?	NO
71	Is sufficient bandwidth available for continuous log ingestion?	YES
72	L1, L2, L3 Analysts, Threat Hunters, IR Leads	Fully Managed
73	Certifications desired (CEH, CompTIA Security+, GCIA, GCIH, etc.)	Industry best
74	Rotational / Fixed / On-call	Fully Managed
75	VPN / Secure jump host / Remote SOC access	VPN
76	Any SOAR platform planned (Splunk Phantom, XSOAR, Siemplify)?	Industry best
77	Integration needed with ITSM or SIEM dashboards?	ITSM
78	Any requirement for ML-based detection / anomaly detection?	YES
79	Email, SMS, Teams, Slack, PagerDuty	YES
80	Who will own SOC operations (CISO, SOC Manager, MSSP)?	SOC Manager
81	Expected deliverables: Playbooks, SOPs, Monthly Reports, RCA	Playbooks, SOPs, Monthly Reports, RCA
82	Frequency of governance reviews (weekly, monthly, quarterly)	Weekly or monthly

83	Who will receive alerts and reports?	we will define in detail engineering

All other terms and conditions of the Inquiry/RFQ remain unchanged.

Regards,

Sun Petrochemicals Pvt. Ltd.