2024

RajCOMP Info Services Limited (RISL)

RFP for Upgradation of Security Operation Center for Govt. of Rajasthan.

Request for Proposal (RFP) Document for Setting up Next Generation Security Operation Center for Govt. of Rajasthan

Mode of Bid Submission	Online though e-Procurement/ e-Tendering system at https://eproc.rajasthan.gov.in
Procuring Authority	Managing Director, RISL First Floor, C-Block, Yojana Bhawan, Tilak Marg, C-Scheme, Jaipur-302005 (Rajasthan)
Last Date & Time of Submission of Bid	As per NIB
Date & Time of Opening of Technical Bid	As per NIB

Name of the Bidding Company/ Firm:			
Contact Person(Authorised Bid Signatory):			
Correspondence Address:			
Mobile No.		**Telephone & Fax Nos.:**	
Website & E-Mail:			

RajCOMP Info Services Limited (RISL)
First Floor, Yojana Bhawan, C-Block, Tilak Marg, C-Scheme, Jaipur-302005 (Raj.)
Phone: 0141- 5103902 Fax: 0141-2228701
Web: http://risl.rajasthan.gov.in

Table of Contents

ABBREVIATIONS & DEFINITIONS

Act	The Rajasthan Transparency in Public Procurement Act, 2012 (Act No. 21 of 2012) and Rules thereto
APT	Advanced Persistent Threat
ADC	Analog-to-Digital Converter
Authorised Signatory	The bidder's representative/ officer vested (explicitly, implicitly, or through conduct) with the powers to commit the authorizing organization to a binding agreement. Also called signing officer/ authority having the Power of Attorney (PoA) from the competent authority of the respective Bidding firm.
BG	Bank Guarantee
BFSI	Banking, Financial Services, and Insurance
Bid/ eBid	A formal offer made in pursuance of an invitation by a procuring entity and includes any tender, proposal or quotation in electronic format
Bid Security	A security provided to the procuring entity by a bidder for securing the fulfilment of any obligation in terms of the provisions of the bidding documents.
Bidding Document	Documents issued by the procuring entity, including any amendments thereto, that set out the terms and conditions of the given procurement and includes the invitation to bid
BoM	Bill of Material
BoQ	Bill of Quantity
CIS	Center for Internet Security
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CEH	Certified Ethical Hacker
CHFI	Computer Hacking Forensic Investigator
CISSP	Certified Information Systems Security Professional
CompTIA CySA+	CompTIA Cybersecurity Analyst+
CMC	Contract Monitoring Committee
Competent Authority	An authority or officer to whom the relevant administrative or financial powers have been delegated for taking decision in a matter relating to procurement. Chairman cum Managing Director, RISL in this bidding document.
Contract/ Procurement Contract	A contract entered into between the procuring entity and a successful bidder concerning the subject matter of procurement
GIAC	Global Information Assurance Certification
GCIH	GIAC Certified Incident Handler Certification
GSEC	GIAC Security Essentials
GMON	GIAC Continuous Monitoring Certification
OSCE	Offensive Security Certified Expert

OSCP	OffSec Certified Professional
Project Period	The contract shall commence from the date of agreement till support period.
Day	A calendar day as per GoR/ GoI.
DAM	Database Activity Monitoring
DeitY, GoI	Department of Electronics and Information Technology, Government of India
DoIT&C	Department of Information Technology and Communications, Government of Rajasthan.
ETDC	Electronic Testing & Development Center
FOR/ FOB	Free on Board or Freight on Board
GoI/ GoR	Govt. of India/ Govt. of Rajasthan
G2G	Government to Government
G2B	Government to Business
G2E	Government to Enterprise
Goods	All articles, material, commodities, electricity, livestock, furniture, fixtures, raw material, spares, instruments, software, machinery, equipment, industrial plant, vehicles, aircraft, ships, railway rolling stock and any other category of goods, whether in solid, liquid or gaseous form, purchased or otherwise acquired for the use of a procuring entity as well as services or works incidental to the supply of the goods if the value of services or works or both does not exceed that of the goods themselves
GST	Goods & Services Tax
ICT	Information and Communication Technology.
IFB	Invitation for Bids (A document published by the procuring entity inviting Bids relating to the subject matter of procurement and any amendment thereto and includes notice inviting Bid and request for proposal)
INR	Indian Rupee
IPS	Intrusion Prevention System
ISI	Indian Standards Institution
ISO	International Organisation for Standardisation
IT	Information Technology
ITB	Instruction to Bidders
LD	Liquidated Damages
LoI	Letter of Intent
NCB	A bidding process in which qualified bidders only from within India are allowed to participate
NBAD	Network Behavior Anomaly Detection

NeGP	National e-Governance Plan of Government of India, Department of Information Technology (DIT), Ministry of Communications and Information Technology (MCIT), New Delhi.
NCIIPC	National Critical Information Infrastructure Protection Centre
NISG	National Information Security Policy and Guidelines
NIB	Notice Inviting Bid
Notification	A notification published in the Official Gazette
OEM	Original Equipment Manufacturer
MTTR	Mean Time To Repair
NIST	National Institute of Standards and Technology
PAN	Permanent Account Number
PBG	Performance Bank Guarantee
PC	Procurement/ Purchase Committee
Procurement Process	The process of procurement extending from the issue of invitation to Bid till the award of the procurement contract or cancellation of the procurement process, as the case may be
Procurement/ Public Procurement	The acquisition by purchase, lease, license or otherwise of works, goods or services, including award of Public Private Partnership projects, by a procuring entity whether directly or through an agency with which a contract for procurement services is entered into, but does not include any acquisition without consideration, and "procure" or "procured" shall be construed accordingly
Project Site	Wherever applicable, means the designated place or places.
PSD/ SD	Performance Security Deposit/ Security Deposit
Purchaser/ Tendering Authority/ Procuring Entity	Person or entity that is a recipient of a good or service provided by a seller (bidder) under a purchase order or contract of sale. Also called buyer. DoIT&C, GoR in this RFP document.
RISL	RajCOMP Info Services Limited
RSDC	Rajasthan State Data Centre
RajSWAN	Rajasthan State Wide Area Network
RVAT	Rajasthan Value Added Tax
SANS	SysAdmin, Audit, Network, and Security
Services	Any subject matter of procurement other than goods or works and includes physical, maintenance, professional, intellectual, consultancy and advisory services or any service classified or declared as such by a procuring entity and does not include appointment of any person made by any procuring entity
SIEM	Security information and event management
SOAR	Security Orchestration, Automation, and Response
SLA	Service Level Agreement is a negotiated agreement between two parties wherein one is the customer and the other is the service provider.

	It is aa service contract where the level of service is formally defined. In practice, the term em is sometimes used to refer to the contracted delivery time (of the service) or performance.
State Government	Government of Rajasthan (GoR)
State Public Procurement Portal	http://sppp.raj.nic.in
STQC	Standardisation Testing and Quality Certification, Govt. of India
Subject Matter of Procurement	Any item of procurement whether in the form of goods, services or works
TIN	Tax Identification Number
TIP	Threat intelligence platforms
TPA	Third Party Auditors
Telecom Sector	Telecom sector mean licensed entities that own and operate the infrastructure for providing mobile telecommunications services, including voice calls, data, and SMS, as per the Telecom Regulatory Authority of India (TRAI).
VAT/ CenVAT	Value Added Tax/ Central VAT
WAF	Web Application Firewall
WO/ PO	Work Order/ Purchase Order

1. INVITATION FOR BID (IFB)& NOTICE INVITING BID (NIB)

Unique Bid No.: RIS2425GLOB00053

Ref No.: F3.3(521)/RISL/PUR/2024-02449/16277 **Dated:** 20-11-2024

Name & Address of the Procuring Entity	• Name: RajCOMP Info Services Limited (RISL) • Address: First Floor, Yojana Bhawan, C-Block, Tilak Marg, C-Scheme, Jaipur-302005 (Rajasthan)
Name & Address of the Project Officer In-charge (POIC)	• Designation: SA (Joint Director), DoIT&C • Address: First Floor, Yojana Bhawan, C-Block, Tilak Marg, C-Scheme, Jaipur-302005 (Rajasthan) • Email: mukeshks.doit@rajasthan.gov.in
Subject Matter of Procurement	RFP for Setting up Next Generation Security Operation Center for Govt. of Rajasthan
Bid Procedure	Single stage: two part (envelop) open competitive eBid procedure at http://eproc.rajasthan.gov.in
Bid Evaluation Criteria (Selection Method)	Low Cost Based Selection (LCBS) - Lowest evaluated technically responsive bid
Websites for downloading Bidding Document, Corrigendum's, Addendums etc.	• Websites: http://sppp.rajasthan.gov.in, http://eproc.rajasthan.gov.in, , http://risl.rajasthan.gov.in and http://doitc.rajasthan.gov.in • Bidding document fee: Rs. 5,000/- (Rupees Five Thousand only) in the form of Cash/Demand Draft / Banker's Cheque/Online Payment in the name of Managing Director, RISL payable at Jaipur. In case of SSI/MSME bid fees shall be 50 % of above specified rates. • RISL Processing Fee: Rs. 2,500/- (Rupees Two Thousand and Five Hundred only) through single challan on e-GRAS as per F.D. circular no. F.6(5)Finance/GF&AR/2018 dated 27-04-2020 or in the form of Demand Draft / Banker's Cheque/ Online Payment in the name of Managing Director, RISL payable at Jaipur.
Estimated Procurement Cost	Rs.95.00 Cr (Rupees Ninety Five Crore Only) (Incl. all Taxes and levies)
Bid Security and Mode of Payment	• Amount (INR): 2% of the estimated procurement cost, 0.50% for S.S.I. unit of Rajasthan, 1.0% for Sick Industries, other than S.S.I., whose cases are pending with Board of Industrial & Financial Reconstruction **OR** As per government Prevailing rules and regulations.f • Mode of Payment: Banker's Cheque or Demand Draft or Bank Guarantee, in specified format, of a Scheduled Bank in favour of "Managing Director, RISL" payable at "Jaipur".

Period of Sale of Bidding Document (Start/ End Date)	From 20-11-2024 (06:00PM) to 03.02.2025 (up to 03:00PM)
Date/ Time/ Place of Pre-bid Meeting	• Date: 03-12-2024, 11:30AM • Place: RSDC, First Floor, Yojana Bhawan, C-Block, Tilak Marg, C-Scheme, Jaipur-302005 (Rajasthan) • Pre-requisite: Submission of tender fees as mentioned Pre-Bid query submission upto Date: 05-12-2024
Manner, Start/ End Date for the submission of Bids	• Manner: Online at eProc website (http://eproc.rajasthan.gov.in) • Start Date: 23.01.2025 (06:00PM) End Date: 03.02.2025 (upto 03:00PM)
Submission of Banker's Cheque/ Demand Draft for Tender Fee, Bid Security, and Processing Fee*	Till End Date: Upto 03:30PM on 03.02.2025
Date/ Time/ Place of Technical Bid Opening	• Date: 03.02.2025 • Time: 04:00PM Place: RSDC, First Floor, Yojana Bhawan, C-Block, Tilak Marg, C-Scheme, Jaipur-302005 (Rajasthan)
Date/ Time/ Place of Financial Bid Opening	Will be intimated later to the Technically qualified bidders
Bid Validity	180 days from the bid submission deadline

Note:

1) Bidder (authorised signatory) shall submit their offer on-line in Electronic formats both for technical and financial proposal. However, DD for Tender Fees, RISL Processing Fees and Bid Security should be submitted physically at the office of Tendering Authority as prescribed in NIB and scanned copy of same should also be uploaded along with the technical Bid/ cover.
2) * In case, any of the bidders fails to physically submit the Banker's Cheque/ Demand Draft for Tender Fee, Bid Security, and RISL Processing Fee up to date/time mentioned in NIT, its Bid shall not be accepted. The Banker's Cheque/ Demand Draft for Bidding document fee, RISL Processing Fee and Bid Security should be drawn in favour of "Managing Director, RajCOMP Info Services Ltd." payable at "Jaipur" from any Scheduled Commercial Bank.
3) To participate in online bidding process, Bidders must procure a Digital Signature Certificate (Type III) as per Information Technology Act-2000 using which they can digitally sign their electronic bids. Bidders can procure the same from any CCA approved certifying agency, i.e. TCS, Safecrypt, Ncode etc. Bidders who already have a valid Digital Signature Certificate (DSC) need not procure a new DSC. Also, bidders must register on

http://eproc.rajasthan.gov.in (bidders already registered on http://eproc.rajasthan.gov.in before 30-09-2011 must register again).

4) RISL will not be responsible for delay in online submission due to any reason. For this, bidders are requested to upload the complete bid well advance in time so as to avoid 11th hour issues like slow speed; choking of web site due to heavy load or any other unforeseen problems.
5) Bidders are also advised to refer "Bidders Manual Kit" available at e-Procurement website for further details about the e-Tendering process.
6) Training for the bidders on the usage of e-Tendering System (e-Procurement) is also being arranged by RISL, GoR on a regular basis. Bidders interested for training may contact e-Procurement Cell, RISL for booking the training slot.
   Contact No: 0141-4022688 (Help desk 10 am to 6 pm on all working days)
   e-mail: eproc@rajasthan.gov.in
   Address : e-Procurement Cell, RISL, YojanaBhawan, Tilak Marg, C-Scheme, Jaipur
7) The procuring entity reserves the complete right to cancel the bid process and reject any or all of the Bids.
8) No contractual obligation whatsoever shall arise from the bidding document/ bidding process unless and until a LoI has been issued or a formal contract is signed and executed between the procuring entity and the successful bidder.
9) Procuring entity disclaims any factual/ or other errors in the bidding document (the onus is purely on the individual bidders to verify such information) and the information provided therein are intended only to help the bidders to prepare a logical bid-proposal.
10) The provisions of RTPP Act, 2012 and Rules, 2013 thereto shall be applicable for this procurement. Furthermore, in case of any inconsistency in any of the provisions of this bidding document with the RTPP Act 2012 and Rules thereto, the later shall prevail.
11) The sale of bidding documents shall be commenced from the date of publication of Notice Inviting Bids (NIB) and shall be stopped one day prior to the date of opening of Bid. The complete bidding document shall also be placed on the State Public Procurement Portal and e-Procurement portal. The prospective bidders shall be permitted to download the bidding document from the websites and pay its price while submitting the Bid to the procuring entity.
12) Bidding documents purchased by Principal of any concern may be used by its authorised sole selling agents/ marketing agents/ distributors/ sub-distributors and authorised dealers or vice versa.

-sd-
SA (Joint Director)

2. PROJECT PROFILE &BACKGROUND INFORMATION

1) Project Profile

a. Government of Rajasthan aims to utilize the benefits of Information Technology to bring about radical changes in the way various processes are carried out presently to improve the Accountability, Transparency & Effectiveness in Government administration. The ultimate objective is to arm the Government with IT enabled systems to assist them in carrying out their day-to-day functions to help deliver G2G, G2B and G2E services.

b. RajComp Info Services Ltd. is State level implementing agency for various flagship core IT infrastructure Projects of the State namely few; RSDC, RajSWAN, RajNet, Multi-layered Security Framework etc.

c. Multi-layered security framework at RSDC is presently catering to security requirements of RSDC and all the networks (SecLAN, RajSWAN, RajNet, etc.) aggregating at RSDC, Jaipur. With all the security devices/ tools in places at RSDC Jaipur, dedicated team is monitoring the security operations.

The details of major existing security infrastructure is mentioned below for ready reference:

i. SIEM
ii. APT
iii. Security Analytics/ Forensics
iv. WAF & DAM
v. NBAD
vi. Zonal & Perimeter Firewalls
vii. Web Security
viii. ADC
ix. IPS
x. Mail Security

d. In view of the emerging threat landscape, it has been decided to upgrade the existing SOC v2.0 in a more structured manner. Hence, RISL intends to invite proposals from organsiations having specfic expertise in SOC domain for upgrading SOC v2.0 in Rajasthan State Data Center P-IV, Jaipur, Rajasthan.

e. The proposed SOC would specifically focus on cyber threats monitoring, investigation, automation, incident management and response, threat intel (third-party), dark web monitoring, DNS Security, reporting etc. under the umbrella of an overall security operations environment and clear executive support.

f. The core objective of SOC upgrade would be to provide centralized capabilities to detect, identify, and respond to security incidents plus service availability that may impact GoR's IT infrastructure, services, and customers. The primary function would be to detect and contain attacks and intrusions, if any, in the shortest possible timeframe, limiting the potential impact and/ or damage that an incident may have by providing near real-time monitoring and analysis of suspicious events.

3. QUALIFICATION/ ELIGIBILITY CRITERIA

1) A bidder (Manufacturer, Dealers & Distributors are eligible to participate in the bidding process) participating in the procurement process shall possess the following minimum qualification/ eligibility criteria.

S. No.	Basic Requirement	Specific Requirements	Documents Required
1.	Legal Entity	The bidder should be a Proprietorship firm duly registered either under the Rajasthan Shops & Commercial Establishments Act, 1958 or any other Act of State/ Union, as applicable for dealing in the subject matter of procurement. (Note: A self-certified declaration regarding the non-applicability of registration to any Act should be submitted by the bidder) **OR** A company registered under Indian Companies Act, 1956 or Companies Act, 2013 **OR** A partnership firm registered under Indian Partnership Act, 1932. Note: Consortium is not allowed.	Copy of valid Registration Certificates OR Copy of Certificates of incorporation.
2.	Financial: Turnover from IT/ ITeS	Average Annual Turnover of the bidder from IT/ITeS for last three financial years, i.e., 2021-22, 2022-23 & 2023-24 should be at least Rs. **500 Crores**.	CA Certificate with CA's Registration Number/ Seal bearing UDIN
3.	Financial: Net Worth	The net worth of the bidder, should be Positive for the last 03 (three) financial years i.e. 2021-22, 2022-23 & 2023-24.	CA Certificate with CA's Registration Number/ Seal bearing UDIN
4.	Technical Capability - I	The bidder must have successfully completed or partially completed *one work order / Contract* of establishment or upgradation of Cyber Security Operation Centre of the value not less than the amount of Rs.80 Crore for any **Government/ BFSI/ PSU/ Telecom sector companies** in India from 01/04/2019 onwards **OR**	Work Order+ Copy AND Work Completion Certificates from Client (In case project is ongoing, satisfactory performance certificate must clearly state the amount for work completed in terms of rupees from Client is to be submitted)

S. No.	Basic Requirement	Specific Requirements	Documents Required
		The bidder must have successfully completed or partially completed *two work order/ contracts* of establishment or upgradation of Cyber security operation centre of the value not less than the amount of Rs. 45 Crore for any **Government/ BFSI/ PSU/ Telecom sector companies** in India from 01/04/2019 onwards. **Note:** The SOC contract/work order is elaborated as it must have supply, implementation & maintenance of SIEM and at least 3 or more tools / technologies which have been asked in this RFP along with SOC services to monitor, prevent, detect, investigate and respond to cyber threats, threat hunting, forensic, incident response, etc.	Note: In case, the Bidder has executed work orders/ Purchase Orders which are meeting the Relevant project experience requirement specified in this item but is unable to share the copy of Work Order/Purchase Order due to binding of Non-Disclosure Agreement (NDA) signed with the Purchaser. The Bidder shall furnish the following document: a) The certificate issued by the Company Secretary / CA of the Bidder clearly specifying nature of work, components & services supplied/provided, date of Work Order/Purchase Order, value of items which are meeting the Relevant Project Experience criteria & status of implementation etc. (+ The date of such work orders should from 01/04/2019 onwards)
5.	Technical Capability -II	The bidder must have successfully completed or shall be in process to implement a Captive SOC solution with 60,000 EPS capacity for at least one client in India belonging to the Government, BFSI, PSU, or Telecom sectors utilizing a "Gartner Magic Quadrant Leader" SIEM solution from 01/04/2019 onwards. Note: In case the bidder in the process of implementing a Captive SOC with 60,000 EPS capacity. The bidder must have successfully completed a Captive SOC	Work Order + Copy + Gartner Magic Quadrant for SIEM. AND Work Completion Certificates from Client (In case project is ongoing, satisfactory performance certificate from Client is to be submitted) Note: In case, the Bidder has executed work orders/ Purchase

S. No.	Basic Requirement	Specific Requirements	Documents Required
		solution with 40,000 EPS capacity for at least one client in India belonging to the Government, BFSI, PSU, or Telecom sectors utilizing a "Gartner Magic Quadrant Leader" SIEM solution from 01/04/2019 onwards.	Orders which are meeting the Relevant project experience requirement specified in this item but is unable to share the copy of Work Order/Purchase Order due to binding of Non-Disclosure Agreement (NDA) signed with the Purchaser. The Bidder shall furnish the following document: a) The certificate issued by the Company Secretary / CA of the Bidder clearly specifying nature of work, components & services supplied/provided, date of Work Order/Purchase Order, value of items which are meeting the Relevant Project Experience criteria & status of implementation etc.
6.	Manpower Capability	Minimum 75 Cyber Security Professional must be available with Bidder on their permanent payroll having any of the below security certification: CISSP/CISA/OSCP/OSCE/GSEC/CHFI/ GMON/ CompTIA CSA+ /GCIH/CEH/ CISM / SIEM. Note: a. For CEH maximum 5 number of certified resources will be considered. b. For one resource only one certification will be considered. Eg. If person 'A' has CISSP, CEH certifications it will be considered as one count.	Undertaking on Bidder Letter Head duly signed & stamp by Company Secretary/ HR.
7.	Tax registration	The bidder should have a registered number of	Copies of relevant certificates of registration

S. No.	Basic Requirement	Specific Requirements	Documents Required
		i. GST ii. Income Tax / Pan number.	
8.	Certifications	The bidder must possess at the time of bidding, following valid certifications: - • ISO 9001:2008 or latest • ISO 27001:2013 or latest	Copy of relevant Certificates/ Documents
9.	Mandatory Undertaking	As per Annexure-5: Self-Declaration	A Self Certified letter
10.	Manufacture Authorization Form (MAF)	MAF is required at the time of Bid Submission.	OEM certified MAF as per Annexure-6

2) Any bidder participating in the procurement process shall -
   a. Possess the necessary professional, technical, financial and managerial resources and competence required by the bidding documents, pre-qualification documents or bidder registration documents, as the case may be.
   b. Not be insolvent, in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and must not be the subject of legal proceedings for any of the foregoing reasons.
   c. Not have, and their directors and officers not have been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of three years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings;
   d. A bidder should not have a conflict of interest in the procurement in question as stated in rule 81 and the bidding documents. The procuring entity shall take appropriate actions against the bidder in accordance with section 11 and Chapter IV of the Act, if it determines that a conflict of interest has flawed the integrity of any procurement process.
   e. The bidder has to be a company/proprietor/LLP or partnership firm/ Society/Corporation/ Board etc. registered for this purpose under any Law/Act of Govt. of India/ Govt. of State. Supporting documentary evidence (Certificate of incorporation/ Registration, etc.) need to be enclosed.
   f. A bidder debarred under section 46 shall not be eligible to participate in any procurement process undertaken by,- (a) any procuring entity, if debarred by the State Government; and (b) a procuring entity if debarred by such procuring entity.
   g. In case of procurement of goods, bidder must be a manufacturer, distributor or bona-fide dealer/ authorized reseller in the goods and it shall furnish necessary proof for the same . Where applicable, proof of authorisation by the manufacturer or country distributor in India, shall be enclosed.

h. Any other eligibility crieteria like Experiance, Turnover, Profitability, Networth etc. may be incorporated taking in view the requirement of project or procurement subject.
i. Bidders are advised that RISL reserves the right to request additional evidence or information from any bidder at any stage of the evaluation process, including during or after the bidding period. This may include, but is not limited to, requests for documentation to verify qualifications, experience, or other criteria specified in the bid documents; clarifications on proposed solutions, methodologies, technologies, or specifications; and supporting documentation to substantiate any claims made by the bidder.

3) In addition to the provisions regarding the qualifications of the bidders as set out in (1,2) above: -
   a. the procuring entity shall disqualify a bidder as per the provisions under "Clause: Exclusion/ Disqualification of bids in Chapter-5: ITB"; and
   b. the procuring entity may require a bidder, who was qualified, to demonstrate its qualifications again in accordance with the same criteria used to qualify such bidder. The procuring entity shall disqualify any bidder that fails to demonstrate its qualifications again, if requested to do so. The procuring entity shall promptly notify each bidder requested to demonstrate its qualifications again as to whether or not the bidder has done so to the satisfaction of the procuring entity.

4. SCOPE OF WORK, DELIVERABLES AND TIMELINES

1) Details of Work (SoW)

A. **Phase-I: Delivery**

I. The Delivery phase would commence from the date of work order.

II. The successful bidder, hereinafter referred to as System Integrator (SI), during this phase, shall arrange the deliver of below items at the RSDC-Jaipur and DR-Jodhpur as per technical specification mentioned in the Annexure-2:-

S. No.	Item	Qty required at BSDC Jaipur	Qty required at DR-Jodhpur
1.	Security Orchestration, Automation & Response (SOAR) Solution with Threat Intelligence Platform (TIP)	1 Nos.	NA
2.	Network Behavior Anomaly Detection (NBAD)/NDR	1 Nos.	NA
3.	DNS Security solution	1 Nos.	NA
4.	Anti-Advanced Persistent Threats solution (APT)	1 Nos.	1 Nos.
5.	A. SIEM with UEBA	1 Nos	NA
	B. Network forensic (Packet Capture and Re-Construction Capability)	2 Nos.	1 Nos.
6.	A. WAF with API Security	1 Nos.	1 Nos.
	B. DAM	1 Nos.	NA

III. The bidder shall promptly submit the delivery challan of all the items mentioned in "Annexure-1: Bill of Material" and "Annexure-2: Technical Specifications" in the time-schedule mentioned at "Project Activity, Deliverables & Timelines" of this bidding document.

B. **Phase-II: Supply and Installation**

The RSOC should have following major technologies and related services with deep learning, analytics, automation of routine SOC activities to improve threat detection and response capabilities leveraging AI/ML –

i. Security Information and Event Management (SIEM)
ii. User and Entity Behavior Analytics (UEBA)
iii. Network forensic (Packet Capture and Re-Construction Capability)
iv. Security Orchestration, Automation and Response (SOAR)
v. Threat Intelligence Platform(TIP)
vi. Web Application Firewall (WAF)
vii. API Security
viii. Database Activity Monitoring (DAM)
ix. Network Behavior Anomaly Detection (NBAD)
x. Unified Threat Intelligence Platform (UIP)
xi. Anti-Advanced Persistent Threats (APT)

xii. DNS Security
xiii. Incident Response Services

b) Bidder shall be required to supply, installation, integration, and commissioning of all Hardware (H/W) and Software (S/W) components as detailed in Annexure-1: Bill of Material and Technical Specifications. The successful bidder will be responsible for providing on-site resources to operate and maintain the supplied systems for a period of three (3) years from the date of Go-Live.

c) Apart from the supplied Technology/ Tools, the manpower deployed by bidder shall be operating/ monitoring the existing/to be deployed security devices infrastructure in R-SOC for overall SOC operations.

d) The bidder shall ensure the availability of a minimum required manpower, including a dedicated Project Manager, throughout all project phases: Design, Deployment, and User Acceptance Testing (UAT). Furthermore, the same core team members shall be retained for the subsequent Operations and Maintenance (O&M) phase at BSDC Jaipur.

e) The specifications given are minimum. Bidders can quote equivalent or higher technical specifications to meet the requirements of RISL. The RFP scope of work and annexures together constitute the overall requirements of the solution.

f) Bidder has to quote for highest/ premium support available from the OEM along with the documentation/ datasheet specifying the details of all the deliverables like service part code, features, etc. for all the OEMs.

g) The bidder shall make sure that the data or logs which are not required for security monitoring, threat detection, threat hunting, compliance, etc. create filtering policies at the data collection layer and make sure it is not counted for license to use the platform optimally and effectively.

h) "The RSOC solution proposed by the bidder must incorporate technologies that leverage self-learning capabilities and advanced analytics models driven by Artificial Intelligence (AI) and Machine Learning (ML). The solution should be architected to handle exceptionally high Input/Output Operations Per Second (IOPS) demands, as outlined in the peak/sizing requirements specified within the scope of work and Annexure-1."

i) Technologies deployed in the R-SOC should collaborate with each other on the real-time basis without manual intervention to leverage strengths of each other for studied analytics, correlation, reporting incidents and maintain overall false positive alerts within the threshold.

j) Security orchestration, automations and response (SOAR) solution should bring down the MTTR / manual efforts and shorten the time to resolve and investigate incidents. SOAR should integrate with all R-SOC and IT asset management components to ensure automation, governance, workflow etc. across all the R-SOC solutions and IT Infrastructure as per requirement.

k) SOAR platform maybe positioned as end to end incident management, Incident response, incident remediation, investigation platform and single evidence repository by the bidder and OEM. Platform should be capable to provide detailed post incident documentation about all the actions taken, root cause, controls implemented etc.

l) A single unified dynamic dashboard specially designed or customised for the RISL with all R-SOC technologies converging together should be provided to the R-SOC. This dashboard should give clear security posture of the data centers to the top Management, CISO and SOC Head, etc.

m) Bidder and OEMs should mandatorily ensure to collaborate with all necessary third parties & other OEMs. Any customization, enhancement and other device/solution administration related activity required in solution to deliver seamless, fully functional integration, custom and native parsers, connectors, incidents management and related workflows, native and custom playbooks, alerts fine tuning, notifications, dashboards, reporting, customization of default templates, additional remediation efforts etc. without any extra charges to the RISL during the Contract period.

n) The supplied softwares (whereever applicable) should include appropriate number of genuine OEM perpetual licenses (as applicable as per OEM licensing policy).

o) All the licenses provided as part of BoM should strictly adhere to requirements of the RFP. If during the Contract period, it is observed by the RISL that provided licenses are not adhering to the RFP requirements then all the additional hardware/software/licenses should be provided and configured without any additional cost to the RISL.

p) The solution must be entirely on-premises. All the features requested in the RFP, with the exception of Unified Intelligence Platform, Threat Intel feeds, and IR Services, shall operate within the on-premises environment without the need for any external internet or cloud connectivity. Internet access will be permitted for the following purposes, adhering to the state data center policy:
   - Signature updates
   - Hotfix application
   - System upgrades
   - Accessing native threat intelligence feeds, etc.

q) The SI will provide weekly progress updates to RISL, discussing the governance structure and project milestones.

List of activities to be performed as part of scope of work by the bidder:

I.Planning

a) Kick-off Meeting:
   Initiate the project with a kick-off meeting to align all stakeholders, clarify objectives, scope, deliverables, and establish expectations for the project.

b) Assessment of Current Architecture:
   Review the existing infrastructure at DOIT&C data centers, including hardware,

network setup, and security tools, to understand the current environment and identify areas for improvement.

c) Review of Security Environment and Guidelines:
Analyze DOIT&C existing security policies, procedures, and compliance standards to ensure they align with the project's objectives and address any gaps.

d) Identify Business and Technical Requirements:
Gather business objectives and technical specifications from stakeholders to ensure the new SOC meets both operational goals and technical needs.

e) Define Prerequisites:
Identify any prerequisites, including hardware, software, or external services, required for successful SOC implementation.

f) Implementation Strategy and Plan:
Develop a detailed implementation plan with clear timelines, milestones, and phases for the project's entire duration, ensuring all steps are well-defined and achievable.

g) Ensure Compatibility and Interoperability:
Confirm that new security solutions will work seamlessly with DOIT&C existing infrastructure and tools to avoid compatibility issues.

h) Resource Allocation:
Define the resources required, including personnel, equipment, and software tools, to support the project's implementation and ongoing operations.

i) Device Placement Strategy:
Plan for the optimal placement of security devices and appliances, following industry best practices for effective monitoring and threat detection.

j) Cross-Departmental Workshops:
Organize workshops with DOIT&C Stakeholders and vendors to cover areas such as solution engineering, gap analysis, asset protection (crown jewels), integration, rule creation, and use case development.

k) Use Case Workshop:
Host a workshop led by the OEM to review existing use cases, develop new ones based on the latest threat intelligence, and align them with frameworks such as MITRE ATT&CK and CIS. Prioritize use cases for implementation and determine data sources and required events for optimal detection.

l) Threat Landscape and Recommendations:
Analyze top threats based on industry trends and attack patterns, and provide actionable recommendations to address these risks in DOIT&C SOC setup.

II Designing:

Architecture of the proposed solutions will be developed within the overall design of the existing data center, taking into account already deployed security solutions. The HLD & LLD will incorporate the integration of these existing security components along with new security solutions being procured as part of this RFP.

- OEM professional services to design the architecture following industry best

practices and would document the same.

- OEM professional services of each technology will provide High-Level Design (HLD) and Low-Level Design (LLD) documents.These designs will consider the technologies being procured within this RFP and integrate seamlessly with the existing security infrastructure (e.g., firewalls, IPS, DDoS, EDR, Email Security,etc.).
- A connectivity and data flow diagram will be developed for each in-scope solution to ensure clear understanding of how data will move through the system.
  - The Detailed Design Document shall include the following aspects:
    i. Technical objectives and requirement fulfilment.
    ii. High-level and low-level solution design.
    iii. Recommendations and best practices
    iv. Proposed network, Security topology and Architecture.
    v. Network - Logical and Physical topology.
    vi. Security design & Ingerations
    vii. Sample configuration templates for hardware devices and other devices for which configurations need to be made.
    viii. Hardware and Software release recommendations based on features and/or functionality.
    ix. Use cases for each of R-SOC solutions.
    x. End-user manuals and SOPs, wherever applicable.

- Detailed solution implementation documentation will be provided to guide the setup, implement and integration of the proposed SOC solutions.
- Business Continuity Planning (BCP), Disaster Recovery (DR), and failover strategies will be documented to ensure system resilience in case of disruptions.
- An Incident Response strategy and process document will be created to outline steps for identifying, responding to, and mitigating security incidents.
- Decommissioning Plan**:**
  - A detailed decommissioning plan will be developed and executed for the existing SOC infrastructure, ensuring a smooth and orderly transition.
  - The decommissioning plan will include procedures for disconnecting devices, decommissioning software licenses, and securely disposing of any sensitive data or equipment.

II.SOC Deployment, Implementation and Integration:

a) Supply and Installation

- The bidder is responsible for supplying and installing appliances and software required for all in-scope solutions, adhering to the architecture design.
- The bidder will be responsible for establishing the SOC in strict adherence to the HLDs and LLDs provided by the OEM professional services.
- Installation includes mounting, labeling, and tagging all equipment properly.The bidder will supply the necessary hardware (servers, storage, switches, passive

cabling, etc.) for the setup at DOIT&C / RISL data centers. RISL will provide the required rack space, cooling, and power supply.

- Acceptance procedures, test cases, and test plans will be developed to verify that the solution meets performance and security requirements.

b) Integration

- Solutions will be integrated with existing infrastructure, including security solutions,servers, network devices, endpoints, and other IT assets.
- The bidder will recommend secure communication methods and assist RISL in defining use cases. All configurations and changes will be documented as part of the policy and process documentation.
- Use cases will undergo the full lifecycle, including creation, testing, fine-tuning of false positives, automation, and notifications.
- The SI will provide detailed documentation on scripts and configurations, including their purpose, functionality, and relevance.

c) User Access and Reporting:

- Enable logging on all provided ICT systems and provide raw logs to the Purchaser.
- Develop a single, unified SOC dashboard with role-based and customized views.
- The dashboard should be organized by context areas such as Security, Business, Control, and Risk, allowing users to access relevant data based on their needs.
- Top Management: Provides an overarching view of the organization's security and business performance, accessible by executive leadership.
- CISO: A comprehensive, detailed dashboard that monitors and presents the organization's overall security posture, leveraging the data collected through the R-SOC.
- Provides an overview of the systems under the administrator’s control, focusing on their operational and security status.
- Displays data specific to the devices and equipment managed by the network or security administrator, including their health, status, and security metrics.
- SLA data should be captured in the dashboard with compliance details.
- SLA reports as agreed upon by RISL should be generated on daily/monthly/quarterly frequency. Exclusive dashboard for uptime / down time of IT Assets, No of Log generated / Analyzed/recommendation etc.
- Daily Report:
    - Top attacker, attacks and attack targets, trends report
    - Top firewall ports access report inbound /outbound)
    - Top signature triggered
    - Top account brute forced
    - Top systems infected
    - Top virus infection in the network
    - Performance report for all solutions in scope
- Weekly Report

- Weekly security incidents status report
- Daily device utilization report
- Device availability report
- Device: Incident, service request and change status report
- weekly threat advisory and vulnerability report
- Top signature triggered
- Top account brute forced
- Top systems infected
- Top virus infection in the network

- Monthly Report
  - Executive summary report for all the services
  - Monthly Security incident status report
  - Monthly security incident trend analysis
  - Monthly device availability report

- Quartely Report
  - Quarterly Security incident status report
  - Quarterly security incident trend analysis
  - Quarterly cyber security activities report
  - Ad-hoc and audit related reports at any frequency desired by RISL

d) **Configuration Management & Security Hardening:**

The solution must adhere to the following security principles:

- Compliance: Configure all solutions according to defined minimum Baseline Security Standards and Security Configuration Documentation, ensuring compliance with industry standards and regulatory guidelines.
- Secure Configuration:
  - Implement and enforce secure configuration standards for all devices, systems, and applications.
  - Conduct regular vulnerability assessments.
  - Ensure timely remediation of all identified vulnerabilities and security misconfigurations.
  - Apply security patches and updates promptly.
  - Implement the principle of least privilege.
- CIS Benchmarks: Ensure compliance with relevant Center for Internet Security (CIS) benchmarks.
- Configuration Baselines:
  - Establish and maintain secure configuration baselines aligned with SANS, NIST, and CIS standards.
  - Regularly review and update baselines to address evolving threats and best practices.
  - Implement continuous monitoring to assess and enforce compliance with established baselines.

- Log Management:
  - Develop and maintain log baselines aligned with NIST or SANS guidelines using SIEM solution, Log management solution would be provided by RISL as a later stage, it should be ingegrated with SIEM solution.
- Documentation:
  - Provide a Minimum Baseline Standard Document or Secure Configuration Document outlining all security requirements.
  - Provide a document outlining access controls and security measures implemented across the solution.
- The bidder may bring own tool or may use open-source tools (such as OpenSCAP, Lynis, Chef InSpec, etc.) for configuration assessment, benchmarking, security hardening and compliance verification. However, they must be able to migrate to RISL's implmented solution at a later stage within mutually agreed timelines and without any additional cost to RISL.

e) Develop Security Playbooks :

- Create and implement security playbooks for handling various threats and incidents, ensuring a well-defined and efficient response process.
- Incident Investigation SOPs: Develop Standard Operating Procedures (SOPs) for conducting in-depth investigations of security incidents, breaches, and service requests to ensure thorough analysis and resolution.
- Reporting and Analysis : Prepare SOPs for generating detailed investigation reports, including root cause analysis (RCA), to identify the underlying causes of security issues.
- Regularly produce security monitoring reports, alert reports, and other necessary documentation to track system performance and security posture.

f) Forensics and Evidence Management:

Develop and Implement Standard Operating Procedures (SOPs) for:

- Conducting forensic analysis on devices and systems to preserve digital evidence for reported/identified incidents.
- Forensic analysis tools: The selected bidder may bring own tool or may utilize open-source forensic analysis tools (such as Volatility, Rekall, FTK, etc.). RISL implements and will provide its own forensic tools to the selected bidder at a later stage. The use of any forensic tools, whether open-source or commercial, will be strictly in accordance with approved Standard Operating Procedures (SOPs).

g) Optimizing & Deployment Validation:

- Solutions will be fine-tuned to meet technical specifications, ensuring a false positive rate of no more than 10% after one year.
- The implemented solution will undergo rigorous validation and certification by the respective OEM Professional Services, adhering to industry best practices. This assessment will include a comprehensive review to ensure the solution meets all defined requirements.

- If any discrepancies or issues are identified during this process, the OEM will provide a detailed report with specific recommendations for corrective actions. The SI is responsible for implementing the necessary changes to address all identified issues and achieve successful certification.
- Successful completion of this rigorous assessment and the implementation of all recommended changes are prerequisites for final sign-off and acceptance of the solution.

III.Migration:

Upon successful "Go-Live" of the upgraded Security Operations Center (SOC), the existing SOC will be decommissioned as per decommission plan. The following activities will be transitioned as per below:

- **SIEM Log Retention and Archiving:**
  - Upon the go-live of the new SIEM solution, all logs will be captured and stored within the new system.
  - The existing SIEM solution will be maintained solely for the retrieval of historical logs for a period of 180 days following the go-live of the new solution.
- **Incident Ticket Management:**
  - Upon successful "Go-Live", all new tickets will be logged within the new ticket management system.
  - The existing SOAR solution will continue to be used for:
    - Managing all existing open tickets.
    - Retrieving historical ticket data for a period of 180 days.
- **Device Configurations:**
  - Configuration Migration: Existing security device configurations from the legacy SOC will be meticulously migrated to their corresponding counterparts within the new SOC environment.
  - Critical Configurations: This includes the migration of critical security configurations such as:
    - IP blocking lists: Blocking of malicious IP addresses.
    - Domain blacklists: Blocking of malicious domains.
    - Hash lists: Blocking of malicious file hashes.
    - Other relevant security controls.

IV.Ticketing Tool:

a) The bidder shall ensure that for all incident management, change management and problem management of IT infrastructure included in RFP is done through ticketing tool and the same is to be provided by the bidder only.

b) The bidder shall integrate all solutions with the ticketing tool for effective reporting and logging of information security incidents.

c) The bidder shall ensure to track and monitor the closure of information security incidents and escalation of these incidents to appropriate teams/ individuals in RISL if required.

d) The bidder shall ensure that all alerts/offences would be integrated and managed

through the RISL ticketing tool.

e) The bidder should also plan and perform complete migration without any loss of tickets/incidents/artefacts once RISL implements its own Ticketing solution. This migration should be performed within mutually agreed timelines and without any additional cost to RISL.

V.Security Operations:

a) Bidder shall be responsible to develop and maintain Standard Operating Procedures (SOP) based on NIST or Similar other framework with respect to R-SOC day to day operations including but not limited to threat management, alert/incident management, reports & dashboards, forensics infrastructure maintenance, rules creation & fine tuning, install/upgrades, updates, asset Integration, knowledge management, segregation of duties, change management, patch & version management, KPI and KRI to measure SOC performance etc. as per policies of the RISL. Bidder to create and modify SOP as per the requirement of the RISL periodically and from time to time, as applicable. All SOP will be reviewed by the RISL on regularly basis.

b) Post-Deployment Management:
After receiving sign-off from RISL, the bidder will take responsibility for managing and monitoring the deployed solutions. This includes ensuring continuous operation, performance optimization, and regular updates.

c) Ongoing Operations

- The bidder will handle tasks related to continuous monitoring, performance tuning, and maintaining compliance with DoIT&C's policies, industry standards, and regulatory guidelines.
- The bidder will also manage change control processes, incident response, and any necessary upgrades to ensure the solutions remain secure and effective.
- A RACI matrix will be created to clearly define roles and responsibilities for all stakeholders involved in the operation and maintenance of the solutions.

d) Incident Response and Investigation:

- Incident Response :

Promptly address security tickets and incidents, taking both corrective and preventive actions to mitigate risks and minimize impact.

e) **Threat Hunting**:

i. Continuous Monitoring**:** Conduct ongoing and proactive threat hunting activities to identify and respond to potential cyber threats.

ii. Advanced Techniques: Utilize advanced threat hunting techniques, such as:
   - Log analysis and threat intelligence correlation.
   - Network traffic analysis and intrusion detection.
   - Endpoint detection and response (EDR).
   - Security information and event management (SIEM) analysis.
   - Other tools / technoloties available in security operation center.

iii. Incident Response Planning: Develop and maintain an incident response plan

to effectively handle security incidents, including:

- Incident detection and triage.
- Containment and eradication of threats.
- Incident investigation and forensic analysis.
- Post-incident review and remediation.

VI.Compliance:

The selected bidder must adhere to the DoIT&C IT & IS Security Policy, specifically in areas relevant to this Request for Proposal (RFP). Detailed requirements will be provided to the selected bidder. Key compliance areas include adherence to the following Acts, Regulations, and Guidelines:

- Acts, Regulations, and Guidelines:
  - Data Protection Act, 2023
  - Information Technology Act, 2000
  - Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
  - CERT-In Guidelines
  - National Cybersecurity Policy 2020
- Incident Response and Reporting: Follow established incident response protocols, with clear procedures for reporting security incidents in a timely manner.
- Password and Access Management Policies:
  Adhere to strict password policies and access management guidelines, ensuring secure authentication, authorization, and access control.
- Confidentiality, Integrity, and Availability:
  Ensure the confidentiality, integrity, availability, non-repudiation, authenticity, and privacy of all data and information handled under this agreement.
- Background Verification of Personnel:
  Regularly conduct background checks for all personnel deployed by the vendor and provide reports to DoIT&C upon request to maintain security and trust.

VII.Right to Audit :

a) Annual External Audit:

The Service Provider agrees to undergo an annual audit conducted by external, empanelled auditors appointed by DOIT&C, CERT-IN, or any relevant regulatory authority. The audit will cover risk parameters defined by DOIT&C, including IT hardware, software, and services provided to DOIT&C. The Service Provider will cooperate with the audit process and submit the resulting certification to DOIT&C. DOIT&C reserves the right to assess the effectiveness of the Service Provider's security, control, risk management, governance systems, and processes. The Service Provider must provide all necessary information and records during the audit. The cost of the audit will be borne by RISL.

b) Corrective Action for Audit Deficiencies:

If the audit identifies any deficiencies in the Service Provider's risk management or compliance with the agreed parameters, the Service Provider will resolve the issues promptly. The vendor must submit all relevant documentation regarding the resolution to the auditors, who will issue a certification confirming that the deficiencies have been addressed. The Service Provider will bear all costs related to addressing and resolving the audit findings.

c) Provision of Information for Audits:

The Service Provider agrees to provide relevant information and records to auditors, DOIT&C officials, CERT-IN, or any other regulatory authority conducting audits. DOIT&C has the right to request and retain any relevant materials, reports, and findings from audits or reviews undertaken by the Service Provider, including financial, internal control, and security assessments related to the services provided to DOIT&C.

VIII.Documentation:

a) General Documentation Requirements

- All documentation must be provided in properly bound volumes using A4-size sheets.
- Three sets of hard copies and one soft copy (on USB) of the final documentation must be submitted.

b) Documentation Content

- The documentation must include high-level design, detailed design, and configuration details for individual features set on various appliances. It should also cover general testing, scenario-based failover testing, Standard Operating Procedures (SOPs), best practices, and any other relevant materials to fulfill the documentation criteria.
- The bidder is responsible for creating SOPs for all in-scope solutions and processes. These documents should be reviewed and updated semi-annually or whenever there are changes in laws or regulatory requirements.

c) Delivery and Installation Reports

- The vendor must submit Delivery and Installation Reports, including part numbers for all components supplied.
- Warranty certificates and license copies for all items supplied must also be provided.

d) Process Documentation

- The vendor must document all processes related to the R-SOC, including but not limited to: tenant provisioning, implementation, data source onboarding, 24/7 monitoring, threat hunting, incident management, threat intelligence, forensic investigations, severity SLAs, incident response plans, and adherence to regulatory guidelines (such as CERT-In, NISPG, NCIIPC, etc.).
- All process documentation should be included as part of the final submission.

e) Ongoing Documentation Updates

- All documentation created as part of this RFP must be updated annually or

whenever there are changes to regulatory requirements or any other legal requirements.

Phase-III: UAT & Go-Live

a) The bidder shall prepare UAT document comprising of test cases for functional and performance testing. The bidder shall ensure that all the test scenarios are identified and provide comprehensive coverage of all aspects. If any additional test cases are required by the Purchaser, the same shall be included by the SI and the revised UAT document shall be resubmitted to the Purchaser for the signoff. The signed off UAT document shall be used for the tests and the results shall be provided to the Purchaser for acceptance.

b) The UAT process shall incorporate the below indicative list of stages given below:
   (a) Submission of documentations including design, architecture, configuration, troubleshooting, Standard Operating Procedure, test cases, etc.
   (b) Atleast one use case per technology listed in scope of work to be shown live.
   (c) Reporting
   (d) Reviewing
   (e) Sign-off

c) The User Acceptance Testing (UAT) shall be conducted by the bidder, after the installation, commissioning and integration has been completed in accordance with the requirements specified in the RFP in the presence of the members of UAT / FAT committee. bidder shall submit a duly signed UAT report for sign off by the Purchaser.

Phase-IV: SOC Operations & Facility Management

From the "Date of commissioning/Go-Live" of project, The bidder shall deploy on-site technical resources as per Annexure-16 for a period of three (3) years from the date of successful commissioning or as requested. The Maintenance & Support Service shall commence for a period as specified in relevant BoM / technical specifications for all hardware and software products. During this period, the SI shall manage operations for Govt. of Rajasthan broadly based on SOP developed based on NIST Framework (given below) along with providing ATS/AMC for the deployed devices (details follows): -

(a) Provide comprehensive OEM onsite/remote warranty maintenance services for the installed hardware and software. This involves comprehensive maintenance of all installed hardware & software covered under the warranty as per 'Warranty' clause including repairing, replacement of faulty parts, modules, sub-modules, assemblies, sub- assemblies, spares etc. with genuine OEM components to make the system functional/ operational as per SLA. The software supplied shall include all the patches, updates and upgrades for period covered under the warranty as per 'Warranty' clause. SI/ OEM shall intimate the Department whenever such updates/patches/upgrades are launched by OEM and shall share its report promptly on the email provided by the purchaser.

(b) Reconfiguration of equipment's/software installed under the project: Whenever required, the SI/OEM shall reconfigure the equipment /software installed under the project to meet the needs of the RSDC Jaipur & RSDC DR Jodhpur

(c) The bidder will monitor and resolve issues according to the defined SLAs in the RFP.

(d) To ensure efficient utilization and monitoring of EPS, optimizing capacity utilization, ensuring quality of data and system performance is maintained optimal.

(e) Develop the baseline for the level of logs to be enabled across the different components of IT including infrastructure, databases, business applications and devices etc. The log baselines should be in line with global best practices based on NIST or SANS etc.

(f) Perform quarterly gap analysis of current levels of logs enabled in OS, databases, web servers, business applications and devices and entire IT infrastructure & recommend and implement remedial actions.

(g) Securely preserve and maintain baseline repository of all the rules and models on analytical, self-learning, supervised & unsupervised learning and keep track of any changes / modifications.

(h) Create new and customize existing reports, dashboards, rules, queries, user interface in all forms to meet the dynamic requirements of the RISL.

(i) Define formats for MIS reporting that includes daily, weekly and monthly or any periodical or adhoc reports, dashboards as per the RISL requirements.

(j) Transfer the knowledge to the DoIT/RISL employees about day to day operations, system / backend level troubleshooting, dashboarding, creating basic and advanced rules & analytical models, creation and customisation of reports & queries etc.

(k) Conduct periodic health check-up of the R-SOC systems by respective OEMs at least once in every year and share the report with the RISL. The recommendations in the report should be rectifies jointly by SI&OEM within a Two week's time. OEMs to ensure that their respective systems operate efficiently, cohesively without any adverse impact on processing, correlation, alerting, dashboarding etc. as per expectations of the RISL and stipulated in the RFP.

(l) For security monitoring of the R-SOC setup, integrate the complete R-SOC setup

with SIEM, DAM, API Security, Firwall, IPS, NBAD, Network forensic, WAF, e-mail security, SOAR, TIP, etc. and ensure logs are auto-sent to these tools by entire R-SOC setup on real-time basis on 24x7x365 days basis. These tools should automatically & immediately raise the alert to the designated official of the R-SOC, if no log is received for in 15 minutes.

(m) Continuous collaboration with global threat intelligence stakeholder's & perform continuous advanced threat hunting and submit weekly report.

(n) Digital forensic/ Network forensic investigation with complete replay of attack including the ingress and egress of payload. Provide complete insight into "*Who did it, what did happen, when did it happen, where did it happen, how did it happen, whom did it impact*" for each security incident. Automation within each R-SOC technology and collaboration among them will be must to achieve it.

(o) Close every technical vulnerability in the R-SOC setup reported in vulnerability assessment (VA) within stipulated time i.e. critical/high risk vulnerability in 15 days, medium/low risk vulnerability in 30 days from the date of reporting of such vulnerability/ observation being managed / owned for SOC team.

(p) R-SOC solutions should be compatible with IPv6 scheme, and there shall be no functional or performance impact on security monitoring due to switch over to IPv6 schema.

(q) Monitoring of alarm conditions that are the result of correlation, pre-defined statistical violation (or baseline alarming) and other activity related to monitoring threat and inappropriate use cases.

(r) Evaluate and analyse of a pattern that if viewed in isolation (each activity in isolation) would not constitute a threat, but in combination is an anomaly or a threat vector (e.g. statistical pattern defined).

(s) Monitor, detect, prevent and appropriately respond against any known and un-knowns security threat, outliers, bots identification etc.

(t) Detect immediately and report slow, uneven but correlated events adopted by adversaries in APT attacks and provide intelligence to the stakeholders to stop them in future from organized threat actors and adversaries. Omni channel threat detection capability to identify similar threats across DoIT&C/RISL data centers.

(u) Bidder/OEM must brief provide executive summary, presentation before going for any major hardware/firmware/middleware/software version upgrade to cover all new features, functionality and bug fixes that are coming with new version/upgrade.

(v) Bidder should ensure the R-SOC technologies, services are capable & configurable to send logs, data, network traffic, security alerts etc. on demand to regulators like CERT-in, NCIIPC, etc.

(w) The SI resources is permitted to take maximum of 12 leaves in a year with prior permission from PoIC/ Nodal Officer /Designated Official.

(x) In case, more than 3 consecutive leaves are required, SI shall have to deploy a trained substitute resource. If the SI failed to provide the substitute resource, the

period will be treated as absence and penalty will be imposed as mentioned in SLA of Chapter-7.

(y) The deployed technical resources from SI shall provide required technical support for the installed hardware/software/solution/integrated infrastructure and shall be responsible for deploying the latest updates, patches and upgrades as and when released by respective OEM in consultation with the designated officer/ RSDC Team. The technical resources shall carryout day-to-day operations as mentioned in the clause but not limited to it.

General Requirement:

1. Escalation Matrix:
   The vendor must provide an escalation matrix in consultation with DOIT&C for different categories of support calls to ensure timely resolution of issues.
2. Dedicated Support Personnel
   All support personnel must be dedicated resources assigned exclusively to DOIT&C, ensuring consistent and reliable service.
3. Support Personnel Expertise
   Support personnel should be skilled in regular configuration tasks, integration with other log sources, rule and policy creation as per DOIT&C's requirements, administration tasks, patch management, user management, and backup procedures.
4. Troubleshooting and Reporting
   On-site support personnel must be capable of troubleshooting issues, maintaining logs of reported problems, and providing root cause analysis and resolution reports to DOIT&C.
5. Change and Configuration Management
   The vendor must implement proper change, configuration, backup, and security management procedures in alignment with CERT-IN guidelines. These procedures must be documented, followed, and maintained, with a copy submitted to DOIT&C.
6. Reinstallation and Reconfiguration
   On-site support personnel should be able to reinstall or reconfigure security components in the event of system failures, crashes, or upgrades. They should also support any third-party security installations, if applicable.
7. Ticket Management and Remediation
   Support personnel should track and resolve issues raised through the ticketing tool, telephone, or email, providing effective remediation.
8. Product Upgrades
   The vendor is responsible for upgrading products to the latest version, following a risk-based approach. Upgrade procedures must be documented and submitted to DOIT&C for approval before implementation.
9. Business Continuity Implementation
   The vendor must ensure all necessary business continuity implementations are performed for the solutions as required.
10. Root Cause Analysis and Corrective Actions

The vendor must conduct root cause analysis for any incidents, take corrective actions, and provide recommendations for improving policies, procedures, tools, and other aspects. Information must be shared with DOIT&C officials.

11. Alerting for Threats
    The vendor is responsible for notifying DOIT&C officials of any unusual occurrences, threats, or attacks detected in the SOC.
12. Compliance with DOIT&C Policies and Security Standards
    The vendor must comply with the following requirements:
    - DOIT&C has the right to review the vendor's processes and SOPs.
    - DOIT&C can assess the skill sets of vendor resources.
    - Advance notice of deployed resources is required, and a proper handover process must be followed for new personnel.
    - All necessary changes must be made to the security infrastructure in compliance with ISO27001 or other relevant security standards and audit requirements.
13. Additional Notes
    - DOIT&C will not provide telephone connections for onsite support staff.
    - On-site L1 and L2 support personnel may be required to work on weekends, holidays, or beyond office hours with advance notice.

2) Training & Support

As a part of deliverables, the bidder has to provide the following trainings:

The selected bidder will be responsible for providing training to designated DOIT&C personnel for the effective operational management of the Security Operations Center systems. 2 Training in a year will be conducted at DOIT&C's premises for up to 20 participants per session at no additional cost to DOIT&C, These sessions will be a minimum of one day, The training will cover the following modules:

1. Pre-Implementation Training:
   Provide training to DOIT&C personnel/onsite support team on the product architecture, functionality, and design of each solution covered under this RFP.
2. Post-Implementation Training:
   Offer hands-on training to DOIT&C personnel/onsite support team on daily operations, including alert monitoring, policy configuration, rule creation, and report generation for all deployed solutions.
3. Knowledge Transfer After Updates:
   Conduct knowledge transfer sessions after each patch or version update, ensuring that personnel are up-to-date with the latest system changes and features.
4. Joint Training by Bidder and OEM:
   The bidder, along with OEM, will jointly provide training for nominated DOIT&C personnel on each solution specified in the scope of work.
5. Ad-Hoc Training Sessions:

Provide ad-hoc training sessions, as requested by DOIT&C, to familiarize staff with new features or functionalities of the solutions. These sessions will be a minimum of one day, and DOIT&C has the right to request this training at its discretion.

6. Training Materials:
   The bidder will supply detailed training materials for each solution, including documentation on installation, operation, integration, maintenance, troubleshooting, and other relevant areas. Additionally, the bidder will provide three copies of these materials to DOIT&C.
7. Training Costs:
   All out-of-pocket expenses related to the training (e.g., travel, accommodation) will be borne by the selected bidder.

Comprehensive training materials shall be provided to all training participants. The detailed theoretical and hands-on training will be conducted by OEM personnel at the DOIT&C premises. DOIT&C will provide the necessary training facilities. The Bidder shall ensure that the training is delivered professionally by certified and experienced personnel (excluding on-site personnel). The training must utilize appropriate courseware and be conducted in accordance with industry best practices."

3) Project Deliverables, Milestones & Time Schedule – As per chapter 7.1

5. INSTRUCTION TO BIDDERS (ITB)

1) Sale of Bidding/ Tender Documents

a) The sale of bidding documents shall be commenced from the date of publication of Notice Inviting Bids (NIB) and shall be stopped one day prior to the date of opening of Bid. The complete bidding document shall also be placed on the State Public Procurement Portal and e-Procurement portal. The prospective bidders shall be permitted to download the bidding document from the websites and pay its price while submitting the Bid to the procuring entity.

b) The bidding documents shall be made available to any prospective bidder who pays the price for it in cash or by bank demand draft, banker's cheque.

c) Bidding documents purchased by Principal of any concern may be used by its authorised sole selling agents/ marketing agents/ distributors/ sub-distributors and authorised dealers or vice versa.

2) Pre-bid Meeting/ Clarifications

a) Pre-requisite: Submission of tender fees as mentioned in NIB, query

b) Any prospective bidder may, in writing, seek clarifications from the procuring entity in respect of the bidding documents.

c) A pre-bid conference can also be scheduled by the procuring entity to clarify doubts of potential bidders in respect of the procurement and the records of such conference shall be intimated to all bidders and where applicable, shall be published on the respective websites.

d) The period within which the bidders may seek clarifications and the period within which the procuring entity shall respond to such requests for clarifications shall be as under: -

   a. Last date of submitting clarifications requests by the bidder: as per NIB
   b. Response to clarifications by procuring entity: as per NIB

e) The minutes and response, if any, shall be provided promptly to all bidders to which the procuring entity provided the bidding documents, so as to enable those bidders to take minutes into account in preparing their bids and shall be published on the respective websites.

3) Changes in the Bidding Document

a) At any time, prior to the deadline for submission of Bids, the procuring entity can for any reason, whether on its own initiative or as a result of a request for clarification by a bidder, modify the bidding documents by issuing an addendum in accordance with the provisions below.

b) In case, any modification is made to the bidding document or any clarification is issued which materially affects the terms contained in the bidding document, the procuring entity shall publish such modification or clarification in the same manner as the publication of the initial bidding document.

c) In case, a clarification or modification is issued to the bidding document, the procuring entity may, prior to the last date for submission of Bids, extend such time limit in order

to allow the bidders sufficient time to take into account the clarification or modification, as the case may be, while submitting their Bids.

d) Any bidder, who has submitted his Bid in response to the original invitation, shall have the opportunity to modify or re-submit it, as the case may be, within the period of time originally allotted or in such extended time. Provided that the Bid last submitted or the Bid as modified by the bidder shall be considered for evaluation.

4) **Period of Validity of Bids**

a) Bids submitted by the bidders shall remain valid during the period specified in the bidding documents.

b) Prior to the expiry of the period of validity of bids, the procuring entity, in exceptional circumstances, may request the bidders to extend the bid validity period for an additional specified period of time. A bidder may refuse the request and such refusal shall be treated as withdrawal of bid but in such circumstances bid security shall not be forfeited.

c) Bidders that agree to an extension of the period of validity of their bids shall extend or get extended the period of validity of bid securities submitted by them or submit new bid securities to cover the extended period of validity of their bids. A bidder whose bid security is not extended, or that has not submitted a new bid security, is considered to have refused the request to extend the period of validity of its bid.

5) **Format and Signing of Bids**

a) Bidders must submit their bids online at e-Procurement portal i.e. http://eproc.rajasthan.gov.in.

b) All the documents uploaded should be digitally signed with the DSC of authorized signatory.

c) A Single stage-Twopart/ cover system shall be followedfor the Bid: -

a. Technical Bid, includingfee details, eligibility& technical documents
b. Financial Bid

d) The technical bidshall consist of the following documents: -

S. No.	Documents Type	Document Format
Fee Details		
1.	Bidding document Fee (Tender Fee)	Proof of submission (PDF)
2.	RISL Processing Fee (e-Procurement)	Instrument/ Proof of submission (PDF)
3.	Bid Security	Instrument/ Proof of submission (PDF)
Eligibility Documents		
4.	Bidder's Authorisation Certificate along with copy of PoA/ Board resolution stating that Auth. Signatory can sign the bid/ contract on behalf of the firm.	As per Annexure-4 (PDF)
5.	Self-Declaration	As per Annexure-5 (PDF)

6.	All the documents mentioned in the "Eligibility Criteria", in support of the eligibility	As per the format mentioned against the respective eligibility criteria clause (PDF)
Technical Documents		
7.	Annexure-1: Bill of Material	As per Annexure-1 (PDF)
8.	Annexure-2: Technical Specification	As per Annexure-2 (PDF)
9.	Manufacturer's Authorisation Form (MAF)	As per Annexure-6 (Indicative Format) (PDF)
10.	Undertaking on Authenticity of Comp. Equip.	As per Annexure-7 (PDF)
11.	Components Offered + Technical specifications compliance sheet for all items only on OEM Letter Head	As per Annexure-8 (PDF) + Annexure-2 (PDF)

b) Financial bid shall include the following documents: -

S. No.	Documents Type	Document Format
1.	Financial Bid – Cover Letter	On bidder's letter head duly signed by authorized signatory as per Annexure-9 (PDF)
2.	Financial Bid - Format	As per BoQ (.XLS) format available on e-Procurement portal

c) The bidder should ensure that all the required documents, as mentioned in this bidding document, are submitted along with the Bid and in the prescribed format only. Non-submission of the required documents or submission of the documents in a different format/ contents may lead to the rejections of the Bid submitted by the bidder.

6) **Cost & Language of Bidding**

a) The Bidder shall bear all costs associated with the preparation and submission of its Bid, and the procuring entity shall not be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

b) The Bid, as well as all correspondence and documents relating to the Bid exchanged by the Bidder and the procuring entity, shall be written English or Hindi Language. Supporting documents and printed literature that are part of the Bid may be in another language provided they are accompanied by an accurate translation of the relevant passages in English/ Hindi language, in which case, for purposes of interpretation of the Bid, such translation shall govern.

7) **Alternative/ Multiple Bids**

Alternative/ Multiple Bids shall not be considered at all. Also, the bidder shall not quote for multiple brands/ make/ models but only one in the technical Bid and should also mention the details of the quoted make/ model in the "Annexure-9: Components Offered".

8) **Bid Security**

a) In open competitive bidding, two-stage bidding, rate contract, electronic reverse auction, bid security shall be 2% or as specified by the State Government of the estimated value of subject matter of procurement put to bid. In case of Small Scale Industries of Rajasthan it shall be 0.5% of the quantity offered for supply and in case of sick industries, other than Small Scale Industries, whose cases are pending with Board of Industrial and Financial Reconstruction, it shall be 1% of the value of bid. Concessional bid security may be taken from registered bidders as specified by the State Government. Every bidder, if not exempted, participating in the procurement process shall be required to furnish the bid security as specified in the notice inviting bids.

b) In lieu of bid security, a bid securing declaration shall be taken from the-
   a. Departments/Boards of the State Government or Central Government;
   b. Government Companies as defined in clause (45) of section 2 of the Companies Act, 2013;
   c. Company owned or controlled, directly or indirectly, by the Central Government, or by any State Government or Governments, or partly by the Central Government and partly by one or more State Governments which is subject to audit by the Auditor appointed by the Comptroller and Auditor-General of India under sub-section (5) or (7) of section 139 of the Companies Act, 2013;
   d. Autonomous bodies, Registered Societies, Cooperative Societies which are owned or controlled or managed by the State Government or Central Government;
   e. Bidder in procurement related to Panchayat Samiti Nandishala Jan Sahbhagita Yojana or Gram Panchayat Goshala/Pashu Asharya Sthal Jan Sahbhagita Yojana issued by the State Government.

c) Bid security instrument or cash receipt of bid security or a bid securing declaration shall necessarily accompany the sealed bid.

d) Bid security of a bidder lying with the procuring entity in respect of other bids awaiting decision shall not be adjusted towards bid security for the fresh bids. The bid security originally deposited may, however, be taken into consideration in case bids are re-invited.

e) The bid security may be given in the form of cash, a banker's cheque or demand draft or bank guarantee or electronic bank guarantee (e-BG), in specified format, of a scheduled bank or deposit through eGRAS. The bid security must remain valid thirty days beyond the original or extended validity period of the bid.

f) The bidding documents may stipulate that the issuer of the bid security and the confirmer, if any, of the bid security, as well as the form and terms of the bid security, must be acceptable to the procuring entity. In cases of International Competitive Bidding, the bidding documents may in addition stipulate that the bid security shall be issued by an issuer in India.

g) Prior to presenting a submission, a bidder may request the procuring entity to confirm the acceptability of proposed issuer of a bid security or of a proposed confirmer, if required. The procuring entity shall respond promptly to such a request.

h) The bank guarantee or electronic bank guarantee (e-BG) presented as bid security shall be got confirmed from the concerned issuing bank. However, the confirmation of the acceptability of a proposed issuer or of any proposed confirmer does not preclude the

procuring entity from rejecting the bid security on the ground that the issuer or the confirmer, as the case may be, has become insolvent or has otherwise ceased to be creditworthy.

i) The bid security of unsuccessful bidders shall be refunded soon after final acceptance of successful bid and signing of Agreement and submitting performance security.

j) The Bid security taken from a bidder shall be forfeited in the following cases, namely:-
   a. When the bidder withdraws or modifies its bid after opening of bids;
   b. When the bidder does not execute the agreement, if any, after placement of supply / work order within the specified period;
   c. When the bidder fails to commence the supply of the goods or service or execute work as per supply / work order within the time specified;
   d. When the bidder does not deposit the performance security within specified period after the supply / work order is placed; and
   e. If the bidder breaches any provision of code of integrity prescribed for bidders specified in the Act and Chapter VI of these rules.

k) In case of the successful bidder, the amount of bid security may be adjusted in arriving at the amount of the Performance Security, or refunded if the successful bidder furnishes the full amount of performance security.

l) The Bid Security shall promptly be returned after the earliest of the following events, namely:-
   a. The expiry of validity of bid security;
   b. The execution of agreement for procurement and performance security is furnished by the successful bidder;
   c. The cancellation of the procurement process; or
   d. The withdrawal of bid prior to the deadline for presenting bids, unless the bidding documents stipulate that no such withdrawal is permitted.

9) **Deadline for the submission of Bids**

a) Bids shall be received online at e-Procurement portal and up to the time and date specified in the NIB.

b) Normally, the date of submission and opening of Bids would not be extended. In exceptional circumstances or when the bidding document are required to be substantially modified as a result of discussions in pre-bid meeting/ conference or otherwise and the time with the prospective bidders for preparation of Bids appears insufficient, the date may be extended by the procuring entity. In such case the publicity of extended time and date shall be given in the manner, as was given at the time of issuing the original NIB and shall also be placed on the State Public Procurement Portal, if applicable. It would be ensured that after issue of corrigendum, reasonable time is available to the bidders for preparation and submission of their Bids. The procuring entity shall also publish such modifications in the bidding document in the same manner as the publication of initial bidding document. If, in the office of the Bids receiving and opening authority, the last date of submission or opening of Bids is a non-working day, the Bids shall be received or opened on the next working day.

10) **Withdrawal, Substitution, and Modification of Bids**

a) If permitted on e-Procurement portal, a Bidder may withdraw its Bid or re-submit its Bid (technical and/ or financial cover) as per the instructions/ procedure mentioned at e-Procurement website under the section "Bidder's Manual Kit".

b) Bids withdrawn shall not be opened and processes further.

11) **Opening of Bids**

a) The Bids shall be opened by the bid opening & evaluation committee on the date and time mentioned in the NIB in the presence of the bidders or their authorised representatives who choose to be present.

b) The committee may co-opt experienced persons in the committee to conduct the process of Bid opening.

c) The committee shall prepare a list of the bidders or their representatives attending the opening of Bids and obtain their signatures on the same. The list shall also contain the representative's name and telephone number and corresponding bidders' names and addresses. The authority letters, if any, brought by the representatives shall be attached to the list. The list shall be signed by all the members of Bid opening committee with date and time of opening of the Bids.

d) All the documents comprising of technical Bid/ cover shall be opened & downloaded from the e-Procurement website (only for the bidders who have submitted the prescribed fee(s) to RISL).

e) The committee shall conduct a preliminary scrutiny of the opened technical Bids to assess the prima-facie responsiveness and ensure that the: -

   a. bid is accompanied by bidding document fee, bid security or bid securing declaration, and processing fee (if applicable);
   b. bid is valid for the period, specified in the bidding document;
   c. bid is unconditional and the bidder has agreed to give the required performance security; and
   d. other conditions, as specified in the bidding document are fulfilled.
   e. any other information which the committee may consider appropriate.

f) No Bid shall be rejected at the time of Bid opening except the Bids not accompanied with the proof of payment or instrument of the required price of bidding document, processing fee and bid security.

g) The Financial Bid cover shall be kept unopened and shall be opened later on the date and time intimated to the bidders who qualify in the evaluation of technical Bids.

12) **Selection Method:**

a) The selection method is Least Cost Based Selection (LCBS or L1).

13) **Clarification of Bids**

a) To assist in the examination, evaluation, comparison and qualification of the bids, the bid evaluation committee may at its discretion, ask any bidder for a clarification regarding

its bid. The committee's request for clarification and the response of the bidder shall be in writing. If committee is not satisfied with the submited clarification may ask for further clarification from bidder.

b) Any clarification submitted by a bidder with regard to its bid that is not in response to a request by the committee shall not be considered.

c) No change in the prices or substance of the bid shall be sought, offered, or permitted, except to confirm the correction of arithmetic errors discovered by the committee in the evaluation of the financial bids.

d) No substantive change to qualification information or to a submission, including changes aimed at making an unqualified bidder, qualified or an unresponsive submission, responsive shall be sought, offered or permitted.

e) All communications generated under this rule shall be included in the record of the procurement proceedings.

14) **Evaluation & Tabulation of Technical Bids**

a) **Determination of Responsiveness**

a. The bid evaluation committee shall determine the responsiveness of a bid on the basis of biding documents and the provisions of sub-section (2) of section 7.

b. A responsive bid is one that meets the requirements of the bidding documents without material deviation, reservation, or omission where: -

(a) "deviation" is a departure from the requirements specified in the bidding documents;

(b) "reservation" is the setting of limiting conditions or withholding from complete acceptance of the requirements specified in the bidding documents; and

(c) "Omission" is the failure to submit part or all of the information or documentation required in the bidding documents.

c. A material deviation, reservation, or omission is one that,

(a) if accepted, shall:- (i) affect in any substantial way the scope, quality, or performance of the subject matter of procurement specified in the bidding documents; or (ii) limits in any substantial way, inconsistent with the bidding documents, the procuring entity's rights or the bidder's obligations under the proposed contract; or

(b) if rectified, shall unfairly affect the competitive position of other bidders presenting responsive bids.

d. The bid evaluation committee shall examine the technical aspects of the bid in particular, to confirm that all requirements of bidding document have been met without any material deviation, reservation or omission.

e. The procuring entity shall regard a bid as responsive if it conforms to all requirements set out in the bidding documents, or it contains minor deviations that do not materially alter or depart from the characteristics, terms, conditions and other requirements set out in the bidding documents, or if it contains errors or oversights that can be corrected without touching on the substance of the bid.

b) **Non-material Non-conformities in Bids**

a. The bid evaluation committee may waive any non-conformities in the Bid that do not constitute a material deviation, reservation or omission, the Bid shall be deemed to be substantially responsive.
b. The bid evaluation committee may request the bidder to submit the necessary information or document like audited statement of accounts/ CA Certificate, Registration Certificate, VAT/ CST clearance certificate, ISO/ CMMi Certificates, etc. within a reasonable period of time. Failure of the bidder to comply with the request may result in the rejection of its Bid.
c. The bid evaluation committee may rectify non-material nonconformities or omissions on the basis of the information or documentation received from the bidder under (b) above.

c) **Technical Evaluation Criteria**

- Bids shall be evaluated based on the documents submitted as part of technical bid. Technical bid shall contain all the documents as asked in the clause "Format and signing of Bids".
- The Bid Evaluation Committee will carry out a detailed evaluation of the bids in order to determine whether the technical aspects are in accordance with the requirements set forth in the RFP documents.
- In order to facilitate the technical bid evaluation, the technical criteria laid down have been presented in the following table. The marking scheme presented here is an indication of the relative importance of the evaluation criteria. Bidders securing above 75% marks in the technical evaluation will only be considered for further Financial Bid evaluation. Bids, which do not secure the minimum, specified technical score will be considered technically nonresponsive and will not be considered for evaluation.
- Bidders will be evaluated for technical capability to execute the project according to the following criteria:

SN	Technical Evaluation Criteria	Max Marks
1.	Past Experience, Quality certifications and manpower quality of the Bidder	70
2.	Proposed, work-plan, timeline and methodology and its Presentation	30
	Total Marks	100

SN	Technical Evaluation Criteria – Parameters	Maximum Score

1.	Average Annual Turnover of the bidder from IT/ITeS for last three financial years, i.e., 2021-22, 2022-23 & 2023-24: • Greater than INR 900 Crore -> 5 Marks • Greater than INR 750 Crore up to INR 900 Crores -> 3 Marks • Greater than INR 500 Crore up to INR 750 Crores -> 2 Marks (Annual audited balance sheet to be provided as evidence)	05
2.	The bidder should have relevant and similar security operation center / security solutions (excluding MSSP / Shared SOC Center delivery model) implementation/ operational experience in PSU/Government/ /BFSI Sector/ Telecom sector companies from the date of issuance of RFP. • Greater than 7 Years -> 05 Marks • Greater than 5 Years up to 7 Years -> 3 Marks • Greater than 3 Years up to 5 Years -> 2 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	05
3.	The Bidder during the last 7 years preceding to the date of this RFP, must have supplied/ implemented and supported/ maintained in-scope solutions (minimum 4 out of 10 in single Purchase Order) related to this RFP to PSU/ Government/ BFSI Sector across different locations in India. • 1 reference -> 5 Marks • 2 referecne -> 10 Marks • 3 reference -> 15 Marks Maximum of three references to be provided and subject to maximum of 15 marks. (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	15
4.	The Bidder during the last 7 years preceding to the date of this RFP, must have experience in PSU/ Government/BFSI/Telecom Sector Firms for setting up the SIEM OEM (excluding MSSP/ Shared SOC Center delivery model) and successful running/ supporting the operations. • Each reference of 60,000 EPS / 1740 GB per day and above -> 5 Marks • Each reference of 50,000 EPS / 1450 GB per day and above -> 4 Marks • Each reference of 40,000 EPS / 1160 GB per day and above -> 3 Marks • Each reference of 30,000 EPS / 870 GB per day and above -> 2 Marks Maximum of three references to be provided and subject to maximum of 15 marks. (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	15

5.	The Bidder during the last 7 years preceding to the date of this RFP, must have supplied/ implemented and supported/ maintained WAF solution to clients in the PSU/Government/BFSI Sector Firms/ Telecom sector companies in India for minimum of: • 3 references and above -> 10 Marks • 2 references and above -> 5 Marks (Supporting Document: Bidder (SI) should provide Copy of the Purchase order/Work order/engagement letter along with invoices and/or Certificate of completion of the work)	10
7.	The OEM for SOAR must have supplied on-prem SOAR solution in BFSI/ PSU/ Telecom sector companies/ Government entities in India. • For 4 and above clients with minimum 5 Analyst/ User licenses -> 10 marks • For 3 clients with minimum 4 Analyst/ User licenses -> 6 marks • For 2 clients with minimum 4 Analyst/ User licenses -> 4 marks	10
8.	The bidder should have a minimum of 75 cyber security resources, having graduation or higher on their payroll, with certification in CISSP/ GCFA/ GCIH/ GCFE/ CHFI/ ECSA/ CREST/ CISM/ CISA/ OSCP/ CCNP Security/ CompTIA Security+ / CEH. (a) >100: 10 Marks. (b) >75 and <100: 7 Marks (c) 75: 5 Marks a. For CEH maximum 5 number of certified resources will be considered. b. For one resource only one certification will be considered. Eg. If person 'A' has CISSP, CEH certifications it will be considered as one count. (Supporting Document: Undertaking on bidder letter head needs to submit along with certification details and relevant evidence).	10

9.	Presentation to be made by the Bidder on understanding of RISL requirements and proposed methodology including but not limited to: • Understanding of the objectives of the project: The extent to which the Bidder's approach and work plan respond to the objectives indicated in the Statement/Scope of Work • Ease of transition, implementation and rollout • Ease of integration with existing & new log sources spread across multiple locations • Experience and expertise in implementation of similar projects of same size • Monitoring, Incident, Response & Remediation Capabilities • Implementation strategy to ensure minimum False positives • Project Governance and Proposed Team structure, their expertise and certifications. (60 Minutes presentation and demonstration of solutions functionalities)	30
Total		100

Note - All the bidders who qualified in pre-qualification criteria (as per chapter-3) and secure a Technical Score of 75 or more will be declared as technically qualified

d) Tabulation of Technical Bids
   a. If Technical Bids have been invited, they shall be tabulated by the bid evaluation committee in the form of a comparative statement to evaluate the qualification of the bidders against the criteria for qualification set out in the bidding document.
   b. The members of bid evaluation committee shall give their recommendations below the table as to which of the bidders have been found to be qualified in evaluation of Technical Bids and sign it.

e) The number of firms qualified in technical evaluation, if less than three and it is considered necessary by the procuring entity to continue with the procurement process, reasons shall be recorded in writing and included in the record of the procurement proceedings.

f) The bidders who qualified in the technical evaluation shall be informed in writing about the date, time and place of opening of their financial Bids.

15) **Evaluation & Tabulation of Financial Bids**

Subject to the provisions of "Acceptance of Successful Bid and Award of Contract" below, the procuring entity shall take following actions for evaluation of financial Bids:-

a) For two part/ coverBid system, the financial Bids of the bidders who qualified in technical evaluation shall be opened online at the notified time, date and place by the bid evaluation committee in the presence of the bidders or their representatives who choose to be present>;

b) the process of opening of the financial Bids shall be similar to that of technical Bids.

c) the names of the bidders, the rates given by them and conditions put, if any, shall be read out and recorded;
d) conditional Bids are liable to be rejected;
e) the evaluation shall include all costs and all taxes and duties applicable to the bidder as per law of the Central/ State Government/ Local Authorities, and the evaluation criteria specified in the bidding documents shall only be applied;
f) the offers shall be evaluated and marked L1, L2, L3 etc. L1 being the lowest offer and then others in ascending order in case price is the only criteria, or evaluated and marked H1, H2, H3 etc. in descending order. <In case quality is also a criteria and the combined score of technical and financial evaluation is considered>;
g) the bid evaluation committee shall prepare a comparative statement in tabular form in accordance with rulesalong with its report on evaluation of financial Bids and recommend the lowest offer for acceptance to the procuring entity, if price is the only criterion, or most advantageous Bid in other case;
h) The members of bids evaluation committee shall give their recommendations below the table regarding lowest Bid or most advantageous Bid and sign it.
i) it shall be ensured that the offer recommended for sanction is justifiable looking to the prevailing market rates of the goods, works or service required to be procured.

16) **Correction of Arithmetic Errors in Financial Bids**

The bid evaluation committee shall correct arithmetical errors in substantially responsive bids, on the following basis, namely: -

a) if there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail and the total price shall be corrected, unless in the opinion of the bid evaluation committee there is an obvious misplacement of the decimal point in the unit price, in which case the total price as quoted shall govern and the unit price shall be corrected;
b) if there is an error in a total corresponding to the addition or subtraction of subtotals, the sub totals shall prevail and the total shall be corrected; and
c) if there is a discrepancy between words and figures, the amount in words shall prevail, unless the amount expressed in words is related to an arithmetic error, in which case the amount in figures shall prevail subject to clause (a) and (b) above.

17) **Price / Purchase Preference In Evaluation**

Price and/ or purchase preference notified by the State Government (GoR) and as mentioned in the bidding document shall be considered in the evaluation of Bids and award of contract.

In case of MSMEs, purchase preference notified by the State Government shall be considered in the evaluation of bids and award of contract.

18) **Negotiations**

a) Except in case of procurement by method of single source procurement or procurement by competitive negotiations, to the extent possible, no negotiations shall be conducted

after the pre-bid stage. All clarifications needed to be sought shall be sought in the pre-bid stage itself.

b) Negotiations may, however, be undertaken only with the lowest or most advantageous bidder when the rates are considered to be much higher than the prevailing market rates.

c) The bid evaluation committee shall have full powers to undertake negotiations. Detailed reasons and results of negotiations shall be recorded in the proceedings.

d) The lowest or most advantageous bidder shall be informed in writing either through messenger or by registered letter and e-mail (if available). A minimum time of seven days shall be given for calling negotiations. In case of urgency the bid evaluation committee, after recording reasons, may reduce the time, provided the lowest or most advantageous bidder has received the intimation and consented to regarding holding of negotiations.

e) Negotiations shall not make the original offer made by the bidder inoperative. The bid evaluation committee shall have option to consider the original offer in case the bidder decides to increase rates originally quoted or imposes any new terms or conditions.

f) In case of non-satisfactory achievement of rates from lowest or most advantageous bidder, the bid evaluation committee may choose to make a written counter offer to the lowest or most advantageous bidder and if this is not accepted by him, the committee may decide to reject and re-invite Bids or to make the same counter-offer first to the second lowest or most advantageous bidder, then to the third lowest or most advantageous bidder and so on in the order of their initial standing and work/ supply order be awarded to the bidder who accepts the counter-offer. This procedure would be used in exceptional cases only.

g) In case the rates even after the negotiations are considered very high, fresh Bids shall be invited.

19) **Exclusion of Bids/ Disqualification**

a) A procuring entity shall exclude/ disqualify a Bid, if: -

   a. the information submitted, concerning the qualifications of the bidder, was false or constituted a misrepresentation; or
   b. the information submitted, concerning the qualifications of the bidder, was materially inaccurate or incomplete; and
   c. the bidder is not qualified as per pre-qualification/ eligibility criteria mentioned in the bidding document;
   d. the Bid materially departs from the requirements specified in the bidding document or it contains false information;
   e. the bidder, submitting the Bid, his agent or any one acting on his behalf, gave or agreed to give, to any officer or employee of the procuring entity or other governmental authority a gratification in any form, or any other thing of value, so as to unduly influence the procurement process;
   f. a bidder, in the opinion of the procuring entity, has a conflict of interest materially affecting fair competition.

b) A Bid shall be excluded/ disqualified as soon as the cause for its exclusion/ disqualification is discovered.

c) Every decision of a procuring entity to exclude a Bid shall be for reasons to be recorded in writing and shall be: -
   a. communicated to the concerned bidder in writing;
   b. published on the State Public Procurement Portal, if applicable.

20) **Lack of competition**

a) A situation may arise where, if after evaluation of Bids, the bid evaluation committee may end-up with one responsive Bid only.In such situation, the bid evaluation committee would check as to whether while floating the NIB all necessary requirements to encourage competition like standard bid conditions, industry friendly specifications, wide publicity, sufficient time for formulation of Bids, etc were fulfilled. If not, the NIBwould be re-floated after rectifying deficiencies. The bid process shall be considered valid even if there is one responsive Bid, provided that: -
   a. the Bid is technically qualified;
   b. the price quoted by the bidder is assessed to be reasonable;
   c. the Bid is unconditional and complete in all respects;
   d. there are no obvious indicators of cartelization amongst bidders; and
   e. the bidder is qualified as per the provisions of pre-qualification/ eligibility criteria in the bidding document
b) The bid evaluation committee shall prepare a justification note for approval by the next higher authority of the procuring entity, with the concurrence of the accounts member.
c) In case of dissent by any member of bid evaluation committee, the next higher authority in delegation of financial powers shall decide as to whether to sanction the single Bid or re-invite Bids after recording reasons.
d) If a decision to re-invite the Bids is taken, market assessment shall be carried out for estimation of market depth, eligibility criteria and cost estimate.

21) **Acceptance of the successful Bid and award of contract**

a) The procuring entity after considering the recommendations of the bid evaluation committee and the conditions of Bid, if any, financial implications, trials, sample testing and test reports, etc., shall accept or reject the successful Bid. If any member of the bid evaluation committee, has disagreed or given its note of dissent, the matter shall be referred to the next higher authority, as per delegation of financial powers, for decision.
b) Decision on Bids shall be taken within original validity period of Bids and time period allowed to procuring entity for taking decision. If the decision is not taken within the original validity period or time limit allowed for taking decision, the matter shall be referred to the next higher authority in delegation of financial powers for decision.
c) Before award of the contract, the procuring entity shall ensure that the price of successful Bid is reasonable and consistent with the required quality.
d) A Bid shall be treated as successful only after the competent authority has approved the procurement in terms of that Bid.
e) The procuring entity shall award the contract to the bidder whose offer has been determined to be the lowest or most advantageous in accordance with the evaluation

criteria set out in the bidding document and if the bidder has been determined to be qualified to perform the contract satisfactorily on the basis of qualification criteria fixed for the bidders in the bidding document for the subject matter of procurement.

f) Prior to the expiration of the period of bid validity, the procuring entity shall inform the successful bidder, in writing, that its Bid has been accepted.

g) As soon as a Bid is accepted by the competent authority, its written intimation shall be sent to the concerned bidder by registered post or email and asked to execute an agreement in the format given in the bidding documents on a non-judicial stamp of requisite value and deposit the amount of performance security or a performance security declaration, if applicable, within a period specified in the bidding documents or where the period is not specified in the bidding documents then within fifteen days from the date on which the letter of acceptance or letter of intent is dispatched to the bidder.

h) If the issuance of formal letter of acceptance is likely to take time, in the meanwhile a Letter of Intent (LOI) may be sent to the bidder. The acceptance of an offer is complete as soon as the letter of acceptance or letter of intent is posted and/ or sent by email (if available) to the address of the bidder given in the bidding document. Until a formal contract is executed, the letter of acceptance or LOI shall constitute a binding contract.

i) The bid security of the bidders who'sBids could not be accepted shall be refunded soon after the contract with the successful bidder is signed and its performance securityis obtained.

22) **Information and publication of award**

Information of award of contract shall be communicated to all participating bidders and published on the respective website(s) as specified in NIB.

23) **Procuring entity's right to accept or reject any or all Bids**

The Procuring entity reserves the right to accept or reject any bid, and to annul the bidding process and reject all bids at any time prior to award of contract, without thereby incurring any liability to the bidders.

24) **Right to vary quantity**

a) If the procuring entity does not procure any subject matter of procurement or procures less than the quantity specified in the bidding documents due to change in circumstances, the bidder shall not be entitled for any claim or compensation except otherwise provided in the bidding documents.

b) Orders for extra items may be placed by the procuring entity in accordance with the Schedule of Powers as prescribed by the Finance Department, upto 5% of the value of the original contract.

c) Orders for additional quantities may be placed on the rates and conditions given in the contract and the original order was given after inviting open competitive bids. Delivery or completion period may also be proportionately increased. The limits of orders for additional quantities shall be as under :-

a. 50% of the quantity of the individual items and 50% of the value of original contract in case of works; and

b. 50% of the value of goods or services of the original contract.

25) **Price Fall**

If the bidder i.e. rate contract holder quotes/ reduces its price to render similar goods, works or services at a price lower than the rate contract price to anyone in the State at any time during the currency of the rate contract, the rate contract price shall be automatically reduced with effect from the date of reducing or quoting lower price, for all delivery of the subject matter of procurement under the rate contract and the rate contract shall be amended accordingly.

26) **Bid Prices/ Comparison Of Rates**

a) Bid prices should be FOR / FOB.

b) Bid prices should be inclusive of all other taxes, levies, octroi , insurance etc. but excluding of GST/CST.

c) The prices under a rate contract shall be subject to price fall clause as per as per Rule 29 (2)(h) of RTPP Rules 2013. Price fall clause is a price safety mechanism in rate contracts and it provides that if the rate contract holder quotes / reduces its price to render similar goods, works or services at a price lower than the rate contract price to anyone in the State at any time during the currency of the rate contract, the rate contract price shall be automatically reduced with effect from the date of reducing or quoting lower price, for all delivery of the subject matter of procurement under that rate contract and the rate contract shall be amended accordingly. The firms holding parallel rate contracts shall also be given opportunity to reduce their price by notifying them the reduced price giving them fifteen days' time to intimate their acceptance to the revised price. Similarly, if a parallel rate contract holding firm reduces its price during currency of the rate contract, its reduced price shall be conveyed to other parallel rate contract holding firms and the original rate contract holding firm for corresponding reduction in their prices. If any rate contract holding firm does not agree to the reduced price, further transaction with it, shall not be conducted.

d) For bids invited for Fixed Quantity as one package the evaluation would be done for all the items of the package put together. The item(s) for which no rates has/have been quoted or left blank would be treated as zero i.e. the bidder will supply these item(s) free of cost and the total amount would be computed accordingly. There is no option with Bidder to submit quote for partial quantity of any items. Procuring Entity will award contract to the lowest priced responsive bidder for this whole package together. Discounts of any kind shall not be considered.

e) For bids invited as item-wise, the bid evaluation would be done for each item separately. There is no option with Bidder to submit quote for particle quantity for any items. If the Bidder does not want to Bid for a particular item, then it should be left blank or filled Zero. Procuring Entity will award the contract for each item separately to the lowest priced responsive bidder for that item. Discounts of any kind shall not be considered.

27) **Risk and Cost**

If the bidder, breaches the contract by failing to deliver goods, services, or works according to the terms of the agreement, the procuring authority may be entitled to terminate the contract and procure the remaining unfinished goods, services, or works through a fresh contractor or by other means, at the risk and cost of the CONTRACTOR. In such cases, the defaulting contractor bears the risk associated with their failure to fulfil their contractual obligations. If the cost of procuring the goods, services, or works from another source is higher than the original contract, the defaulting contractor is liable for the additional cost incurred by the procuring authority. The Risk & Cost amount payable by the contractor or recoveries in lieu of Risk Purchase may be recovered from supplier by encashing/invoking Bank Guarantee, Security Deposits available with PE against the same or any other contract or may be adjusted against dues payable to supplier by PE against other purchase orders/contracts/work orders etc. by any unit/region etc. of PE.

28) **Change In Law**

Unless otherwise specified in the Contract, if after the date of Bid submission, any law, regulation, ordinance, order or byl aw having the force of law is enacted, promulgated, abrogated, or changed in India, where the Site is located (which shall be deemed to include any change in interpretation or application by the competent authorities) that subsequently affects the Delivery Date and/or the Contract Price, then such Delivery Date and/or Contract Price shall be correspondingly increased or decreased, to the extent that the Supplier has thereby been affected in the performance of any of its obligations under the Contract. Notwithstanding the foregoing, such additional or reduced cost shall not be separately paid or credited if the same has already been accounted for in the price adjustment provisions .

29) **Performance Security**

a) Performance security shall be solicited from all successful bidders except the,-
   a. Departments/Boards of the State Government or Central Government;
   b. Government Companies as defined in clause (45) of section 2 of the Companies Act, 2013;
   c. Company owned or controlled, directly or indirectly, by the Central Government, or by any State Government or Governments, or partly by the Central Government and partly by one or more State Governments which is subject to audit by the Auditor appointed by the Comptroller and Auditor-General of India under sub-section (5) or (7) of section 139 of the Companies Act, 2013;
   d. Autonomous bodies, Registered Societies, Cooperative Societies which are owned or controlled or managed by the State Government or Central Government;
   e. Bidder in procurement related to Panchayat Samiti Nandishala Jan Sahbhagita Yojana or Gram Panchayat Goshala/Pashu Asharya Sthal Jan Sahbhagita Yojana issued by the State Government. However, a performance security declaration shall be taken from them. The State Government may relax the provision of performance security in a particular procurement or any class of procurement.

b) The amount of performance security shall be five percent, or as may be specified in the bidding documents, of the amount of supply order in case of procurement of goods and services and ten percent of the amount of work order in case of procurement of works. In case of Small Scale Industries of Rajasthan it shall be one percent of the amount of quantity ordered for supply of goods and in case of sick industries, other than Small Scale Industries, whose cases are pending before the Board of Industrial and Financial Reconstruction (BIFR), it shall be two percent of the amount of supply order.

c) Performance security shall be furnished in any one of the following forms-
   a. deposit though eGRAS;
   b. Bank Draft or Banker's Cheque of a scheduled bank;
   c. National Savings Certificates and any other script/instrument under National Savings Schemes for promotion of small savings issued by a Post Office in Rajasthan, if the same can be pledged under the relevant rules. They shall be accepted at their surrender value at the time of bid and formally transferred in the name of procuring entity with the approval of Head Post Master;
   d. Bank guarantee or electronic bank guarantee (e-BG) of a scheduled bank. It shall be got verified from the issuing bank. Other conditions regarding bank guarantee shall be same as mentioned in the rule 42 for bid security;
   e. Fixed Deposit Receipt (FDR) of a scheduled bank. It shall be in the name of procuring entity on account of bidder and discharged by the bidder in advance. The procuring entity shall ensure before accepting the Fixed Deposit Receipt that the bidder furnishes an undertaking from the bank to make payment/premature payment of the Fixed Deposit Receipt on demand to the procuring entity without requirement of consent of the bidder concerned. In the event of forfeiture of the performance security, the Fixed Deposit shall be forfeited along with interest earned on such Fixed Deposit.
   f. In case of procurement of works, the successful bidder at the time of signing of the contract agreement, may submit option for deduction of performance security from his each running and final bill @ 10% of the amount of the bill.

d) Performance security furnished in the form specified in clause (b) to (e) of sub-rule (3) shall remain valid for a period of sixty days beyond the date of completion of all contractual obligations of the bidder, including warranty obligations and maintenance and defect liability period.

e) **Additional Performance Security**- In addition to Performance Security as specified in rule 75, an Additional Performance Security shall also be taken from the successful bidder in case of unbalanced bid. The Additional Performance Security shall be equal to fifty percent of Unbalanced Bid Amount. The Additional Performance Security shall be deposited in lump sum by the successful bidder before execution of Agreement. The Additional Performance Security shall be deposited through e-Grass, Demand Daft, Banker's Cheque, Government Securities , Bank guarantee or electronic Bank Guarantee (e-BG)

f) Explanation : For the purpose of this rule,- (i) Unbalanced Bid means any bid below more than fifteen percent of Estimated Bid Value. (ii) Estimated Bid Value means value of

subject matter of procurement mention in bidding documents by the Procuring Entity. (iii) Unbalanced Bid Amount means positive difference of eighty five percent of Estimated Bid Value minus Bid Amount Quoted by the bidder.

g) In case of unbalanced bid relating to IT & e-Governance Project having cost of twenty crore rupees or more and approved by the State e-Governance Mission Team (SeMT), Department of Information Technology & Communication, Rajasthan as a High Tech Project, the Additional Performance Security shall not required to be taken.

h) The Additional Performance Security shall be refunded to the contractor after satisfactory completion of the entire work. The Additional Performance Security shall be forfeited by the Procuring Entity when work is not completed within stipulated period by the contractor.

30) **Execution of agreement**

a) A procurement contract shall come into force from the date on which the letter of acceptance or letter of intent is despatched to the bidder.

b) The successful bidder shall sign the procurement contract within 15 days from the date on which the letter of acceptance or letter of intent is despatched to the successful bidder.

c) If the bidder, who'sBid has been accepted, fails to sign a written procurement contract or fails to furnish the required performance security within specified period, the procuring entity shall take action against the successful bidder as per the provisions of the bidding document and Act. The procuring entity may, in such case, cancel the procurement process or if it deems fit, offer for acceptance the rates of lowest or most advantageous bidder to the next lowest or most advantageous bidder, in accordance with the criteria and procedures set out in the bidding document.

d) The bidder will be required to execute the agreement on a non-judicial stamp of specified value at its cost **[As per government Prevailing rules and regulations] and to be purchased from anywhere in Rajasthan only.**

31) **Confidentiality**

a) Notwithstanding anything contained in this bidding document but subject to the provisions of any other law for the time being in force providing for disclosure of information, a procuring entity shall not disclose any information if such disclosure, in its opinion, is likely to: -

   a. impede enforcement of any law;
   b. affect the security or strategic interests of India;
   c. affect the intellectual property rights or legitimate commercial interests of bidders;
   d. affect the legitimate commercial interests of the procuring entity in situations that may include when the procurement relates to a project in which the procuring entity is to make a competitive bid, or the intellectual property rights of the procuring entity.

b) The procuring entity shall treat all communications with bidders related to the procurement process in such manner as to avoid their disclosure to competing bidders or to any other person not authorised to have access to such information.

c) The procuring entity may impose on bidders and sub-contractors, if there are any for fulfilling the terms of the procurement contract, conditions aimed at protecting information, the disclosure of which violates (a) above.
d) In addition to the restrictions specified above, the procuring entity, while procuring a subject matter of such nature which requires the procuring entity to maintain confidentiality, may impose condition for protecting confidentiality of such information.
e) Bidder has to sign Non-Disclosure Agreement with the tendering authority as per indicative format annexed as Annexure -15: Non-Disclosure Agreement.

32) **Cancellation of procurement process**

a) If any procurement process has been cancelled, it shall not be reopened but it shall not prevent the procuring entity from initiating a new procurement process for the same subject matter of procurement, if required.
b) A procuring entity may, for reasons to be recorded in writing, cancel the process of procurement initiated by it -
   a. at any time prior to the acceptance of the successful Bid; or
   b. after the successful Bid is accepted in accordance with (d) and (e) below.
c) The procuring entity shall not open any bids or proposals after taking a decision to cancel the procurement and shall return such unopened bids or proposals.
d) The decision of the procuring entity to cancel the procurement and reasons for such decision shall be immediately communicated to all bidders that participated in the procurement process.
e) If the bidder who'sBid has been accepted as successful fails to sign any written procurement contract as required, or fails to provide any required security for the performance of the contract, the procuring entity may cancel the procurement process.
f) If a bidder is convicted of any offence under the Act, the procuring entity may: -
   a. cancel the relevant procurement process if the Bid of the convicted bidder has been declared as successful but no procurement contract has been entered into;
   b. rescind (cancel) the relevant contract or forfeit the payment of all or a part of the contract value if the procurement contract has been entered into between the procuring entity and the convicted bidder.

33) **Code of Integrity for Bidders**

a) No person participating in a procurement process shall act in contravention of the code of integrity prescribed by the State Government.
b) The code of integrity include provisions for: -
   a. Prohibiting
      i. any offer, solicitation or acceptance of any bribe, reward or gift or any material benefit, either directly or indirectly, in exchange for an unfair advantage in the procurement process or to otherwise influence the procurement process;
      ii. any omission, including a misrepresentation that misleads or attempts to mislead so as to obtain a financial or other benefit or avoid an obligation;

iii. any collusion, bid rigging or anti-competitive behaviour to impair the transparency, fairness and progress of the procurement process;
iv. improper use of information shared between the procuring entity and the bidders with an intent to gain unfair advantage in the procurement process or for personal gain;
v. any financial or business transactions between the bidder and any officer or employee of the procuring entity;
vi. any coercion including impairing or harming or threatening to do the same, directly or indirectly, to any party or to its property to influence the procurement process;
vii. any obstruction of any investigation or audit of a procurement process;

b. disclosure of conflict of interest;
c. disclosure by the bidder of any previous transgressions with any entity in India or any other country during the last three years or of any debarment by any other procuring entity.

c) Without prejudice to the provisions below, in case of any breach of the code of integrity by a bidder or prospective bidder, as the case may be, the procuring entity may take appropriate measures including: -
a. exclusion of the bidder from the procurement process;
b. calling-off of pre-contract negotiations and forfeiture or encashment of bid security;
c. forfeiture or encashment of any other security or bond relating to the procurement;
d. recovery of payments made by the procuring entity along with interest thereon at bank rate;
e. cancellation of the relevant contract and recovery of compensation for loss incurred by the procuring entity;
f. debarment of the bidder from participation in future procurements of the procuring entity for a period not exceeding three years.

Without prejudice to the provisions of Chapter IV of the Act, in case of breach of any provision of the code of integrity by a bidder or prospective bidder, as the case may be, the procuring entity may take appropriate action in accordance with the provisions of subsection (3) of section 11 and section 46.

34) **Conflict Of Interest**

(1) A conflict of interest for bidders is considered to be a situation in which a party has interests that could improperly influence that party's performance of official duties or responsibilities, contractual obligations, or compliance with applicable laws and regulations.

(2) A Bidder may be considered to be in conflict of interest with one or more parties in a bidding process if, including but not limited to:-

(a) They have controlling partners in common;

(b)They receive or have received any direct or indirect subsidy from any of them;

(c) They have the same legal representative for purposes of the bid;

(d)They have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about or influence on the bid of another;

(e) A bidder participates in more than one bid in the same bidding process. However, this does not limit the inclusion of the same sub-contractor, not otherwise participating as a bidder, in more than one bid; or

(f) A bidder or any of its affiliates participated as a consultant in the preparation of the design or technical specifications of the subject matter of procurement of the bidding process. All bidders shall provide in Qualification Criteria and Biding Forms, a statement that the bidder is neither associated nor has been associated directly or indirectly, with the consultant or any other entity that has prepared the design, specifications and other documents for the subject matter of procurement or being proposed as Project Manager for the contract.

35) **Interference with Procurement Process**

A bidder, who: -

a) withdraws from the procurement process after opening of financial bids;
b) withdraws from the procurement process after being declared the successful bidder;
c) fails to enter into procurement contract after being declared the successful bidder;
d) fails to provide performance security or any other document or security required in terms of the bidding documents after being declared the successful bidder, without valid grounds,

shall, in addition to the recourse available in the bidding document or the contract, be punished with fine which may extend to fifty lakh rupees or ten per cent of the assessed value of procurement, whichever is less.

36) **Appeals**

a) Subject to section 4 of RTPP Act, 2012, if any bidder or prospective bidder is aggrieved that any decision, action or omission of the procuring entity is in contravention to the provisions of this Act or the rules or guidelines issued thereunder, he may file an appeal to such officer of the procuring entity, as may be designated by it for the purpose, within a period of ten days or such other period as may be specified in the pre-qualification documents, bidder registration documents or bidding documents, as the case may be, from the date of such decision or action, omission, as the case may be, clearly giving the specific ground or grounds on which he feels aggrieved:
    a. Provided that after the declaration of a bidder as successful in terms of section 27of RTPP Act, 2012 , the appeal may be filed only by a bidder who has participated in procurement proceedings.
    b. Provided further that in case a procuring entity evaluates the technical bid before the opening of the financial bid, an appeal related to the matter of financial bid may be filed only by a bidder whose technical bid is found to be acceptable.
b) If the officer designated under sub-section (1) fails to dispose of the appeal filed under that sub-section within the period specified in subsection (3), or if the bidder or

prospective bidder or the procuring entity is aggrieved by the order passed under sub section (2), the bidder or prospective bidder or the procuring entity, as the case may be, may file a second appeal to an officer or authority designated by the State Government in this behalf within fifteen days from the expiry of the 31 period specified in sub-section (3) or of the date of receipt of the order passed under sub-section (2), as the case may be.

c) Every appeal shall be accompanied by an order appealed against, if any, affidavit verifying the facts stated in the appeal and proof of payment of fee.
d) Every appeal may be presented to First Appellate Authority or Second Appellate Authority, as the case may be, in person or through registered post or authorised representative.

First Appeallate Authority: Secretary/ Principal Secretary, IT&C, Govt. of Rajasthan
Second Appeallate Authority: Secretary, Finance (Budget) Department, Govt. of Rajasthan.

e) Form of Appeal:
    a. Every appeal under (a) and (c) above shall be as per Annexure-16 along with as many copies as there are respondents in the appeal.
    b. Every appeal shall be accompanied by an order appealed against, if any, affidavit verifying the facts stated in the appeal and proof of payment of fee.
    c. Every appeal may be presented to First Appellate Authority or Second Appellate Authority, as the case may be, in person or through registered post or authorised representative.
f) Fee for Appeal: Fee for filing appeal:
    a. Fee for first appeal shall be rupees two thousand five hundred and for second appeal shall be rupees ten thousand, which shall be non-refundable.
    b. The fee shall be paid in the form of bank demand draft or banker's cheque of a Scheduled Bank payable in the name of Appellate Authority concerned.
g) Procedure for disposal of appeal:
    a. The First Appellate Authority or Second Appellate Authority, as the case may be, upon filing of appeal, shall issue notice accompanied by copy of appeal, affidavit and documents, if any, to the respondents and fix date of hearing.
    b. On the date fixed for hearing, the First Appellate Authority or Second Appellate Authority, as the case may be, shall,-
        i. hear all the parties to appeal present before him; and
        ii. peruse or inspect documents, relevant records or copies thereof relating to the matter.
    c. After hearing the parties, perusal or inspection of documents and relevant records or copies thereof relating to the matter, the Appellate Authority concerned shall pass an order in writing and provide the copy of order to the parties to appeal free of cost.
    d. The order passed under (c) shall also be placed on the State Public Procurement Portal.

h) No information which would impair the protection of essential security interests of India, or impede the enforcement of law or fair competition, or prejudice the legitimate commercial interests of the bidder or the procuring entity, shall be disclosed in a proceeding under an appeal.

i) Whoever intentionally files any vexatious, frivolous or malicious appeal or complaint with the intention of delaying or defeating any procurement or causing loss to any procuring entity or any other bidder, shall be punished with fine which may extend to twenty lakh rupees or five per cent of the value of procurement, whichever is less.

37) **Stay of procurement proceedings**

While hearing of an appeal, the officer or authority hearing the appeal may, on an application made in this behalf and after affording a reasonable opportunity of hearing to the parties concerned, stay the procurement proceedings pending disposal of the appeal, if he, or it, is satisfied that failure to do so is likely to lead to miscarriage of justice.

38) **Vexatious Appeals & Complaints**

Whoever intentionally files any vexatious, frivolous or malicious appeal or complaint under the "The Rajasthan Transparency Public Procurement Act 2012", with the intention of delaying or defeating any procurement or causing loss to any procuring entity or any other bidder, shall be punished with fine which may extend to twenty lakh rupees or five per cent of the value of procurement, whichever is less.

39) **Offenses by Firms/ Companies**

a) Where an offence under "The Rajasthan Transparency Public Procurement Act 2012" has been committed by a company, every person who at the time the offence was committed was in charge of and was responsible to the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of having committed the offence and shall be liable to be proceeded against and punished accordingly:

Provided that nothing contained in this sub-section shall render any such person liable for any punishment if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence.

b) Notwithstanding anything contained in (a) above, where an offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of or is attributable to any neglect on the part of any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of having committed such offence and shall be liable to be proceeded against and punished accordingly.

c) For the purpose of this section-

   a. "company" means a body corporate and includes a limited liability partnership, firm, registered society or co- operative society, trust or other association of individuals; and

b. "director" in relation to a limited liability partnership or firm, means a partner in the firm.

d) Abetment of certain offenses: Whoever abets an offence punishable under this Act, whether or not that offence is committed in consequence of that abetment, shall be punished with the punishment provided for the offence.

40) **Debarment from Bidding**

a) A bidder shall be debarred by the State Government if he has been convicted of an offence
   a. under the Prevention of Corruption Act, 1988 (Central Act No. 49 of 1988); or
   b. under the Indian Penal Code, 1860 (Central Act No. 45 of 1860) or any other law for the time being in force, for causing any loss of life or property or causing a threat to public health as part of execution of a public procurement contract.

b) A bidder debarred under (a) above shall not be eligible to participate in a procurement process of any procuring entity for a period not exceeding three years commencing from the date on which he was debarred.

c) If a procuring entity finds that a bidder has breached the code of integrity prescribed in terms of "Code of Integrity for bidders" above, it may debar the bidder for a period not exceeding three years.

d) Where the entire bid security or the entire performance security or any substitute thereof, as the case may be, of a bidder has been forfeited by a procuring entity in respect of any procurement process or procurement contract, the bidder may be debarred from participating in any procurement process undertaken by the procuring entity for a period not exceeding three years.

e) The State Government or a procuring entity, as the case may be, shall not debar a bidder under this section unless such bidder has been given a reasonable opportunity of being heard.

41) **Monitoring of Contract**

a) An officer or a committee of officers named Contract Monitoring Committee (CMC) may be nominated by procuring entity to monitor the progress of the contract during its delivery period.

b) During the delivery period the CMC shall keep a watch on the progress of the contract and shall ensure that quantity of goods and service delivery is in proportion to the total delivery period given, if it is a severable contract, in which the delivery of the goods and service is to be obtained continuously or is batched. If the entire quantity of goods and service is to be delivered in the form of completed work or entire contract like fabrication work, the process of completion of work may be watched and inspections of the selected bidder's premises where the work is being completed may be inspected.

c) If delay in delivery of goods and service is observed a performance notice would be given to the selected bidder to speed up the delivery.

d) Any change in the constitution of the firm, etc. shall be notified forth with by the contractor in writing to the procuring entity and such change shall not relieve any former member of the firm, etc., from any liability under the contract.

e) No new partner/ partners shall be accepted in the firm by the selected bidder in respect of the contract unless he/ they agree to abide by all its terms, conditions and deposits with the procuring entity through a written agreement to this effect. The bidder's receipt for acknowledgement or that of any partners subsequently accepted as above shall bind all of them and will be sufficient discharge for any of the purpose of the contract.

f) The selected bidder shall not assign or sub-let his contract or any substantial part thereof to any other agency without the permission of procuring entity.

42) **Procurement Governing Act & Rules**

All the provisions and clauses of RTPP Act 2012 and Rules 2013 (as per amended time to time) thereto shall be applicable for this procurement. Furthermore, in case of any inconsistency in any of the provisions of this bidding document with the RTPP Act 2012 and Rules thereto, the later shall prevail. The bidders are advised to adhere the provisions as mentions in RTPP Act 2012 and Rules 2013.

43) **Provision In Conflict**

If a clause or a provision or a term or a condition is in conflict with RTPP Act, 2012 and RTPP Rules, 2013, in this situation, provisions and rules of RTPP Act, 2012 and RTPP Rules, 2013 shall prevail.

6. GENERAL TERMS AND CONDITIONS OF TENDER & CONTRACT

Bidders should read these conditions carefully and comply strictly while sending their bids.

Definitions

For the purpose of clarity, the following words and expressions shall have the meanings hereby assigned to them: -

a) "Contract" means the Agreement entered into between the Purchaser and the successful/ selected bidder, together with the Contract Documents referred to therein, including all attachments, appendices, and all documents incorporated by reference therein.
b) "Contract Documents" means the documents listed in the Agreement, including any amendments thereto.
c) "Contract Price" means the price payable to the successful/ selected bidder as specified in the Agreement, subject to such additions and adjustments thereto or deductions there from, as may be made pursuant to the Contract.
d) "Day" means a calendar day.
e) "Delivery" means the transfer of the Goods from the successful/ selected bidder to the Purchaser in accordance with the terms and conditions set forth in the Contract.
f) "Completion" means the fulfilment of the related services by the successful/ selected bidder in accordance with the terms and conditions set forth in the Contract.
g) "Goods" means all of the commodities, raw material, machinery and equipment, and/or other materials that the successful/ selected bidder is required to supply to the Purchaser under the Contract.
h) "Purchaser" means the entity purchasing the Goods and related services, as specified in the bidding document.
i) "Related Services" means the services incidental to the supply of the goods, such as insurance, installation, training and initial maintenance and other similar obligations of the successful/ selected bidder under the Contract.
j) "Subcontractor" means any natural person, private or government entity, or a combination of the above, including its legal successors or permitted assigns, to whom any part of the Goods to be supplied or execution of any part of the related services is subcontracted by the successful/ selected bidder.
k) "Supplier/ Successful or Selected bidder" means the person, private or government entity, or a combination of the above, whose Bid to perform the Contract has been accepted by the Purchaser and is named as such in the Agreement, and includes the legal successors or permitted assigns of the successful/ selected bidder.
l) "The Site," where applicable, means the designated project place(s) named in the bidding document.

Note: The bidder shall be deemed to have carefully examined the conditions, specifications, size, make and drawings, etc., of the goods to be supplied and related services to be rendered. If the bidder has any doubts as to the meaning of any portion of these conditions or of the specification, drawing, etc., he shall, before submitting the Bid and signing the contract refer the same to the procuring entity and get clarifications.

1) **Contract Documents**

Subject to the order of precedence set forth in the Agreement, all documents forming the Contract (and all parts thereof) are intended to be correlative, complementary, and mutually explanatory.

2) **Interpretation**

a) If the context so requires it, singular means plural and vice versa.

b) Entire Agreement: The Contract constitutes the entire agreement between the Purchaser and the Supplier/ Selected Bidder and supersedes all communications, negotiations and agreements (whether written or oral) of parties with respect thereto made prior to the date of Contract.

c) Amendment: No amendment or other variation of the Contract shall be valid unless it is in writing, is dated, expressly refers to the Contract, and is signed by a duly authorized representative of each party thereto.

d) Non-waiver: Subject to the condition (f) below, no relaxation, forbearance, delay, or indulgence by either party in enforcing any of the terms and conditions of the Contract or the granting of time by either party to the other shall prejudice, affect, or restrict the rights of that party under the Contract, neither shall any waiver by either party of any breach of Contract operate as waiver of any subsequent or continuing breach of Contract.

e) Any waiver of a party's rights, powers, or remedies under the Contract must be in writing, dated, and signed by an authorized representative of the party granting such waiver, and must specify the right and the extent to which it is being waived.

f) Severability: If any provision or condition of the Contract is prohibited or rendered invalid or unenforceable, such prohibition, invalidity or unenforceability shall not affect the validity or enforceability of any other provisions and conditions of the Contract.

3) **Language**

a) The Contract as well as all correspondence and documents relating to the Contract exchanged by the successful/ selected bidder and the Purchaser, shall be written in English language only. Supporting documents and printed literature that are part of the Contract may be in another language provided they are accompanied by an accurate translation of the relevant passages in the language specified in the special conditions of the contract, in which case, for purposes of interpretation of the Contract, this translation shall govern.

b) The successful/ selected bidder shall bear all costs of translation to the governing language and all risks of the accuracy of such translation.

4) **Joint Venture, Consortium or Association**

Joint Venture, Consortium or Association is not allowed for the bid.

5) **Eligible Goods and Related Services**

a) For purposes of this Clause, the term "goods" includes commodities, raw material, machinery, equipment, and industrial plants; and "related services" includes services such as insurance, transportation, supply & installation.

b) All articles/ goods being bid, other than those marked in the Bill of Material (BoM) should be the ones which are produced in volume and are used by a large number of users in India/ abroad. All products quoted by the successful/ selected bidder must be associated with specific make and model number, item code and names and with printed literature describing configuration and functionality. Any deviation from the printed specifications should be clearly mentioned in the offer document by the bidder/ supplier. Also, the bidder is to quote/ propose only one make/ model against the respective item.

c) The OEM/ Vendor/distributor of the quoted product must have its own registered spares depot in India having adequate inventory of the equipment being quoted for providing the necessary spares as per the requirements of this bidding document.

d) The OEM/ Vendor of the quoted product should also have its direct representation in India in terms of registered office for at least past 3 years. The presence through any Distribution/ System Integration partner agreement will not be accepted.

e) Bidder must quote products in accordance with above clause "Eligible goods and related services".

6) **Service of Notice, Documents & Orders**

a) A notice, document or order shall be deemed to be served on any individual by -

   a. delivering it to the person personally; or
   b. leaving it at, or sending it by post to, the address of the place of residence or business of the person last known;
   c. on a body corporate by leaving it at, or sending it by post to, the registered office of the body corporate.

b) When the procedure laid down in (a) above is followed, service shall be deemed to be effected by properly addressing, preparing and posting the document, notice or order, as the case may be.

7) **Scope of Supply**

a) Subject to the provisions in the bidding document and contract, the goods and related services to be supplied shall be as specified in the bidding document.

b) Unless otherwise stipulated in the Contract, the scope of supply shall include all such items not specifically mentioned in the Contract but that can be reasonably inferred from the Contract as being required for attaining delivery and completion of the goods and related services as if such items were expressly mentioned in the Contract.

c) The bidder shall not quote and supply and hardware/ software that is likely to be declared as End of Sale in next 6 months and End of Service/ Support for a period of 5 Years from the last date of bid submission. OEMs are required to mention this in the MAF for all the quoted hardware/ software. If any of the hardware/ software is found to be declared as End of Sale/ Service/ Support, then the bidder shall replace all such

hardware/ software with the latest ones having equivalent or higher specifications without any financial obligation to the purchaser.

8) **Delivery & Installation**

a) Subject to the conditions of the contract, the delivery of the goods and completion of the related services shall be in accordance with the delivery and completion schedule specified in the bidding document. The details of supply/ shipping and other documents to be furnished by the successful/ selected bidder are specified in the bidding document and/ or contract.

b) The contract for the supply can be repudiated at any time by the purchase officer, if the supplies are not made to his satisfaction after giving an opportunity to the bidder of being heard and recording the reasons for repudiation.

c) The Supplier/ Selected Bidder shall arrange to supply & install the ordered materials/ system as per specifications within the specified delivery/ completion period at various departments and/ or their offices/ locations mentioned in the PO/ WO.

d) Shifting the place of Installation: The user will be free to shift the place of installation within the same city /town/ district/ division. The successful/ selected bidder shall provide all assistance, except transportation, in shifting of the equipment. However, if the city/town is changed, additional charges of assistance in shifting and providing maintenance services for remaining period would be decided mutually.

9) **Supplier's/ Selected Bidder's Responsibilities**

The Supplier/ Selected Bidder shall supply all the goods and related services included in the scope of supply in accordance with the provisions of bidding document and/ or contract.

10) **Purchaser's Responsibilities**

a) Whenever the supply of goods and related services requires that the Supplier/ Selected Bidder obtain permits, approvals, and import and other licenses from local public authorities, the Purchaser shall, if so required by the Supplier/ Selected Bidder, make its best effort to assist the Supplier/ Selected Bidder in complying with such requirements in a timely and expeditious manner.

b) The Purchaser shall pay all costs involved in the performance of its responsibilities, in accordance with the general and special conditions of the contract.

11) **Contract Price**

a) The Contract Price shall be paid as specified in the contract subject to any additions and adjustments thereto, or deductions there from, as may be made pursuant to the Contract.

b) Prices charged by the Supplier/ Selected Bidder for the Goods delivered and the Related Services performed under the Contract shall not vary from the prices quoted by the Supplier/ Selected Bidder in its bid, with the exception of any price adjustments authorized in the special conditions of the contract.

12) **Recoveries from Supplier/ Selected Bidder/Authorised partner**

a) Recoveries of liquidated damages, short supply, breakage, rejected articles shall ordinary be made from bills.

b) Amount may also be withheld to the extent of short supply, breakages, and rejected articles and in case of failure in satisfactory replacement by the supplier along with amount of liquidated damages shall be recovered from his dues and security deposit available with the department.

c) In case, recovery is not possible recourse will be taken under Rajasthan PDR Act or any other law in force.

13) **Taxes & Duties**

a) The TDS, GST (Whichever is applicable) etc., if applicable, shall be deducted at source/ paid by tendering authority as per prevailing rates.

b) For goods supplied from outside India, the successful/ selected bidder shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the country.

c) For goods supplied from within India, the successful/ selected bidder shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Goods to the Purchaser.

d) If any tax exemptions, reductions, allowances or privileges may be available to the successful/ selected bidder in India, the Purchaser shall use its best efforts to enable the successful/ selected bidder to benefit from any such tax savings to the maximum allowable extent.

14) **Sub-contracting**

a) The bidder shall not assign or sub-let his contract or any substantial part thereof to any other agency without the permission of Purchaser/ Tendering Authority.

b) If permitted, the selected bidder shall notify the Purchaser, in writing, of all subcontracts awarded under the Contract, if not already specified in the Bid. Subcontracting shall in no event relieve the Supplier/ Selected Bidder from any of its obligations, duties, responsibilities, or liability under the Contract.

c) Subcontractors, if permitted, shall comply with the provisions of bidding document and/ or contract.

15) **Confidential Information**

a) The Purchaser and the Supplier/ Selected Bidder shall keep confidential and shall not, without the written consent of the other party hereto, divulge to any third party any drawings, documents, data, or other information furnished directly or indirectly by the other party hereto in connection with the Contract, whether such information has been furnished prior to, during or following completion or termination of the Contract.

b) The Supplier/ Selected Bidder may furnish to its Subcontractor, if permitted, such documents, data, and other information it receives from the Purchaser to the extent required for the Subcontractor to perform its work under the Contract, in which event

the Supplier/ Selected Bidder shall obtain from such Subcontractor an undertaking of confidentiality similar to that imposed on the Supplier/ Selected Bidder.

c) The Purchaser shall not use such documents, data, and other information received from the Supplier/ Selected Bidder for any purposes unrelated to the Contract. Similarly, the Supplier/ Selected Bidder shall not use such documents, data, and other information received from the Purchaser for any purpose other than the design, procurement, or other work and services required for the performance of the Contract.

d) The obligation of a party under sub-clauses above, however, shall not apply to information that: -
   i. the Purchaser or Supplier/ Selected Bidder need to share with other institutions participating in the Contract;
   ii. now or hereafter enters the public domain through no fault of that party;
   iii. can be proven to have been possessed by that party at the time of disclosure and which was not previously obtained, directly or indirectly, from the other party; or
   iv. otherwise lawfully becomes available to that party from a third party that has no obligation of confidentiality.

e) The above provisions shall not in any way modify any undertaking of confidentiality given by either of the parties hereto prior to the date of the Contract in respect of the supply or any part thereof.

f) The provisions of this clause shall survive completion or termination, for whatever reason, of the Contract.

16) **Specifications and Standards**

a) All articles supplied shall strictly conform to the specifications, trademark laid down in the bidding document and wherever articles have been required according to ISI/ ISO/ other applicable specifications/ certifications/ standards, those articles should conform strictly to those specifications/ certifications/ standards. The supply shall be of best quality and description. The decision of the competent authority/ purchase committee whether the articles supplied conform to the specifications shall be final and binding on the supplier/ selected bidder.

b) Technical Specifications and Drawings
   i. The Supplier/ Selected Bidder shall ensure that the goods and related services comply with the technical specifications and other provisions of the Contract.
   ii. The Supplier/ Selected Bidder shall be entitled to disclaim responsibility for any design, data, drawing, specification or other document, or any modification thereof provided or designed by or on behalf of the Purchaser, by giving a notice of such disclaimer to the Purchaser.
   iii. The goods and related services supplied under this Contract shall conform to the standards mentioned in bidding document and, when no applicable standard is mentioned, the standard shall be equivalent or superior to the official standards whose application is appropriate to the country of origin of the Goods.

c) Wherever references are made in the Contract to codes and standards in accordance with which it shall be executed, the edition or the revised version of such codes and standards shall be those specified in the bidding document. During Contract execution,

any changes in any such codes and standards shall be applied only after approval by the Purchaser and shall be treated in accordance with the general conditions of the contract.

17) **Packing and Documents**

a) The Supplier/ Selected Bidder shall provide such packing of the Goods as is required to prevent their damage or deterioration during transit to their final destination, as indicated in the Contract. During transit, the packing shall be sufficient to withstand, without limitation, rough handling and exposure to extreme temperatures, salt and precipitation, and open storage. Packing case size and weights shall take into consideration, where appropriate, the remoteness of the final destination of the Goods and the absence of heavy handling facilities at all points in transit.

b) The packing, marking, and documentation within and outside the packages shall comply strictly with such special requirements as shall be expressly provided for in the Contract, including additional requirements, if any, specified in the contract, and in any other instructions ordered by the Purchaser.

18) **Insurance**

a) The goods will be delivered at the destination godown in perfect condition. The Goods supplied under the Contract shall be fully insured against loss by theft, destruction or damage incidental to manufacture or acquisition, transportation, storage, fire, flood, under exposure to weather and delivery at the designated project locations, in accordance with the applicable terms. The insurance charges will be borne by the supplier and Purchaser will not be required to pay such charges if incurred.

b) The goods will be delivered at the FOR destination in perfect condition.

19) **Transportation**

The supplier/ selected bidder shall be responsible for transport by sea, rail and road or air and delivery of the material in the good condition to the consignee at destination. In the event of any loss, damage, breakage or leakage or any shortage the bidder shall be liable to make good such loss and shortage found at the checking/ inspection of the material by the consignee. No extra cost on such account shall be admissible.

20) **Inspection**

a) The Purchase Officer or his duly authorized representative shall at all reasonable time have access to the supplier's/ selected bidder's premises and shall have the power at all reasonable time to inspect and examine the materials and workmanship of the goods/ equipment/ machineries during manufacturing process or afterwards as may be decided. Inspection shall be made at supplier's/ selected bidder's godown at Jaipur (at supplier's/ selected bidder's cost).

b) The supplier/ selected bidder shall furnish complete address of the premises of his factory, office, go-down and workshop where inspection can be made together with name and address of the person who is to be contacted for the purpose.

c) As soon as the goods arrive at the designated place for supply, an inspection Committee constituted by RISL shall inspect the material for its conformity with Technical specification mentioned.
d) After successful inspection, it will be supplier's/ selected bidder's responsibility to dispatch and install the equipment at respective locations without any financial liability to the Purchaser. However, supplies when received at respective locations shall be subject to inspection to ensure whether they conform to the specification.

21) **Samples**

a) When notified by the Purchaser to the supplier/ bidder/ selected bidder, Bids for articles/ goods marked in the BoM shall be accompanied by four sets of samples of the articles quoted properly packed. Such samples if submitted personally will be received in the office. A receipt will be given for each sample by the officer receiving the samples. Samples if sent by train, etc., should be despatched freight paid and the R/R or G.R. should be sent under a separate registered cover. Samples for catering/ food items should be given in a plastic box or in polythene bags at the cost of the bidder.
b) Each sample shall be marked suitably either by written on the sample or on a slip of durable paper securely fastened to the sample, the name of the bidder and serial number of the item, of which it is a sample in the schedule.
c) Approved samples would be retained free of cost upto the period of six months after the expiry of the contract. RISL shall not be responsible for any damage, wear and tear or loss during testing, examination, etc., during the period these samples are retained. The Samples shall be collected by the supplier/ bidder/ selected bidder on the expiry of stipulated period. RISL shall in no way make arrangements to return the samples. The samples uncollected within 9 months after expiry of contract shall be forfeited by RISL and no claim for their cost, etc., shall be entertained.
d) Samples not approved shall be collected by the unsuccessful bidder. RISL will not be responsible for any damage, wear and tear, or loss during testing, examination, etc., during the period these samples are retained. The uncollected samples shall be forfeited and no claim for their cost, etc., shall be entertained.
e) Supplies when received may be subject to inspection to ensure whether they conform to the specifications or with the approved samples. Where necessary or prescribed or practical, tests shall be carried out in Government laboratories, reputed testing house like STQC (ETDC) and the like and the supplies will be accepted only when the articles conform to the standard of prescribed specifications as a result of such tests.
f) The supplier/ selected bidder shall at its own expense and at no cost to the Purchaser carry out all such tests and/ or inspections of the Goods and Related Services as are specified in the bidding document.

22) **Drawl of Samples**

In case of tests, wherever feasible, samples shall be drawn in four sets in the presence of selected bidder or his authorised representative and properly sealed in their presence. Once

such set shall be given to them, one or two will be sent to the laboratories and/ or testing house and the third or fourth will be retained in the office for reference and record.

23) **Testing charges**

Testing charges shall be borne by the Government. In case of test results showing that supplies are not upto the prescribed standards or specifications, the testing charges shall be payable by the selected bidder.

24) **Rejection**

a) Articles not approved during inspection or testing shall be rejected and will have to be replaced by the selected bidder at his own cost within the time fixed by the Purchase Officer.
b) If, however, due to exigencies of RISL's work, such replacement either in whole or in part, is not considered feasible, the Purchase Officer after giving an opportunity to the selected bidder of being heard shall for reasons to be recorded, deduct a suitable amount from the approved rates. The deduction so made shall be final.
c) The rejected articles shall be removed by the supplier/ bidder/ selected bidder within 15 days of intimation of rejection, after which Purchase Officer shall not be responsible for any loss, shortage or damage and shall have the right to dispose of such articles as he thinks fit, at the selected bidder's risk and on his account.

25) **Delivery period & Extent of Quantity – Repeat Orders**

b) The time specified for delivery shall be deemed to be the essence of the contract and the successful bidder shall arrange supplies within the period on receipt of the firm order from the Purchase Officer.
c) The selected bidder shall arrange supplies within the stipulated time period.
d) If the orders are placed in excess of the quantities, the bidder shall be bound to meet the required supply. Repeat orders may also be placed on the rate and conditions given in the bidding document. If the bidder fails to do so, the Purchase Officer shall be fee to arrange for the balance supply by limited tender or otherwise and the extra cost incurred shall be recoverable from the bidder.

26) **Freight**

a) All goods must be sent freight paid through Railways or goods transport. If goods are sent freight to pay the freight together with departmental charge 5% of the freight will be recovered from the supplier's bill.
b) R.R. should be sent under registered cover through Bank only.
c) In case supply is desired to be sent by the purchase officer by passenger train, the entire railway freight will be borne by the bidder.
d) Remittance charges on payment made shall be borne by the bidder.

27) **Payments**

a) Unless otherwise agreed between the parties, payment for the delivery of the stores will be made on submission of bill in proper form by the bidder to the Purchase Officer in accordance with G.F.& A.R all remittance charges will be bourne by the bidder.
b) In case of disputed items, 10% to 25% of the amount shall be withheld and will be paid on settlement of the dispute.
c) Payment in case of those goods which need testing shall be made only when such tests have been carried out, test results received conforming to the prescribed specification.

28) **Liquidated Damages (LD)**

a) In case of extension in the delivery period with liquidated damages the recovery shall be made on the basis of following percentages of value of Stores with the bidder has failed to supply/ install/ complete:-

Sr.	Condition	LD %*
a.	Delay up to one fourth period of the prescribed delivery period & completion of Goods and Services.	2.5 %
b.	Delay exceeding one fourth but not exceeding half of the prescribed delivery period & completion of Goods and Services.	5.0 %
c.	Delay exceeding half but not exceeding three fourth of the prescribed delivery period & completion of Goods and Services.	7.5 %
d.	Delay exceeding three fourth of the prescribed delivery period, & completion of Goods and Services.	10.0 %

b) Fraction of a day in reckoning period of delay in supplies shall be eliminated if it is less than half a day.
c) The maximum amount of liquidated damages shall be 10%. The percentage refers to the payment due for associated milestone.
d) If the supplier requires an extension of time in completion of contractual supply on account of occurrence of any hindrance, he shall apply in writing to the authority, which has placed the supply order, for the same immediately on occurrence of the hindrance but not after the stipulated date of completion of supply.
e) Delivery period may be extended with or without liquidated damages if the delay in the supply of goods is on account of hindrances beyond the control of the bidder.

29) Bidders must make their own arrangements to obtain import licence, if necessary. If a bidder imposes conditions which are in addition to or in conflict with the conditions mentioned herein, his bid is liable to summary rejection. In any case none of such conditions will be deemed to have been accepted unless specifically mentioned in the letter of acceptance of bid issued by the Purchase Officer.

30) **Taxes And Duties**

(1) The TDS, GSTif applicable, shall be deducted at source/ paid by RISL as per prevailing rates.

(2) For goods supplied from outside India, the successful/ selected bidder shall be entirely responsible for all taxes, stamp duties, license fees, and other such levies imposed outside the country.

(3) For goods supplied from within India, the successful/ selected bidder shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Goods to the Purchaser.

(4) If any tax exemptions, reductions, allowances or privileges may be available to the successful/ selected bidder in India, the Purchaser shall use its best efforts to enable the successful/ selected bidder to benefit from any such tax savings to the maximum allowable extent.

31) **Settlement of Disputes:**

a) General: If any dispute arises between the supplier/ selected bidder and RISL during the execution of a contract that should be amicably settled by mutual discussions. However, if the dispute is not settled by mutual discussions, a written representation will be obtained from the supplier/ selected bidder on the points of dispute. The representation so received shall be examined by the concerned Procurement Committee which sanctioned the tender. The Procurement Committee may take legal advice of a counsel and then examine the representation. The supplier/ selected bidder will also be given an opportunity of being heard. The Committee will take a decision on the representation and convey it in writing to the supplier/ selected bidder.

b) Standing Committee for Settlement of Disputes: If a question, difference or objection arises in connection with or out of the contract/ agreement or the meaning of operation of any part, thereof or the rights, duties or liabilities of either party have not been settled by mutual discussions or the decision of tender sanctioning Procurement Committee, it shall be referred to the empowered standing committee for decision, if the amount of the claim is more than Rs. 50,000/-. The empowered standing committee shall consist of following members: - (RISL)

- Chairman of BoD of RISL : Chairman
- Secretary, DoIT&C or his nominee, not below the rank of Deputy Secretary : Member
- Managing Director, RISL : Member
- Director (Technical)/ Executive Director, RISL : Member
- Director (Finance), RISL : Member
- A Legal Expert to be nominated by the Chairman : Member

c) Procedure for reference to the Standing Committee: The supplier/ selected bidder shall present his representation to the Managing Director, RISL along with a fee equal to two percent of the amount of dispute, not exceeding Rupees One Lakh, within one month from the date of communication of decision of the tender sanctioning Procurement Committee. The officer-in-charge of the project who was responsible for taking delivery of the goods and/ or service from the supplier/ selected bidder shall prepare a reply of representation and shall represent the RISL's stand before the standing committee. From the side of the supplier/ selected bidder, the claim case may be

presented by himself or through a lawyer. After hearing both the parties, the standing committee shall announce its decision which shall be final and binding both on the supplier/ selected bidder and RISL. The standing committee, if it so decides, may refer the matter to the Board of Directors of RISL for further decision.

d) Legal Jurisdiction: All legal proceedings arising out of any dispute between both the parties regarding a contract shall be settled by a competent court having jurisdiction over the place, where agreement has been executed and by no other court, after decision of the standing committee for settlement of disputes.

32) All legal proceedings, if necessary arise to institute may by any of the parties (Government of Contractor) shall have to be lodged in courts situated in Rajasthan and not elsewhere.

33) **Jurisdiction**

The jurisdiction in respect of all claims and matters arising under the contract shall be the courts situated in Jaipur, Rajasthan.

34) **Authenticity of Equipment**

a) The selected bidder shall certify (as per Annexure-9) that the supplied goods are brand new, genuine/ authentic, not refurbished, conform to the description and quality as specified in this bidding document and are free from defects in material, workmanship and service.

b) If during the contract period, the said goods be discovered counterfeit/ unauthentic or not to conform to the description and quality aforesaid or have determined (and the decision of the Purchase Officer in that behalf will be final and conclusive), notwithstanding the fact that the purchaser may have inspected and/ or approved the said goods, the purchaser will be entitled to reject the said goods or such portion thereof as may be discovered not to conform to the said description and quality, on such rejection the goods will be at the selected bidder's risk and all the provisions relating to rejection of goods etc., shall apply. The selected bidder shall, if so called upon to do, replace the goods etc., or such portion thereof as is rejected by Purchase Officer, otherwise the selected bidder shall pay such damage as may arise by the reason of the breach of the condition herein contained. Nothing herein contained shall prejudice any other right of the Purchase Officer in that behalf under this contract or otherwise.

c) Goods accepted by the purchaser in terms of the contract shall in no way dilute purchaser's right to reject the same later, if found deficient in terms of the this clause of the contract.

35) **Warranty**

a) The bidder must supply all items with comprehensive on-site OEM warranty valid for a period as mentioned in Annexure-1 of this RFP after the goods, or any portion thereof as the case may be, have been delivered to, installed and accepted at the final destination(s) indicated in the bidding document. However, if delay of installation is

more than a month's time due to the reasons ascribed to the bidder, the warranty shall start from the date of last successful installation of the items covered under the PO.

b) At the time of goods delivery, the selected bidder shall submit a certificate/ undertaking from all the respective OEMs mentioning the fact that the goods supplied are covered under comprehensive warranty & support for the prescribed period.

c) The purchaser shall give a written notice to the selected bidder stating the nature of any defect together with all available evidence thereof, promptly following the discovery thereof. The purchaser shall afford all reasonable opportunity for the selected bidder to inspect such defects. Upon receipt of such notice, the selected bidder shall expeditiously cause to repair the defective goods or parts thereof or replace the defective goods or parts thereof with brand new genuine/ authentic ones having similar or higher specifications from the respective OEM, at no cost to the Purchaser. Any goods repaired or replaced by the selected bidder shall be delivered at the respective location without any additional costs to the purchaser.

d) If having been notified, the selected bidder fails to remedy the defect within the period specified, the purchaser may proceed to take within a reasonable period such remedial action as may be necessary, in addition to other recourses available in terms and conditions of the contract and bidding document.

e) During the warranty period, the bidder shall also be responsible to ensure adequate and timely availability of spare parts needed for repairing the supplied goods.

36) **Patent Indemnity**

a) The supplier/ selected bidder shall, subject to the Purchaser's compliance with sub-clause (b) below, indemnify and hold harmless the Purchaser and its employees and officers from and against any and all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which the Purchaser may suffer as a result of any infringement or alleged infringement of any patent, utility model, registered design, trademark, copyright, or other intellectual property right registered or otherwise existing at the date of the Contract by reason of: -

   i. the installation of the Goods by the supplier/ selected bidder or the use of the Goods in the country where the Site is located; and

   ii. the sale in any country of the products produced by the Goods.

   Such indemnity shall not cover any use of the Goods or any part thereof other than for the purpose indicated by or to be reasonably inferred from the Contract, neither any infringement resulting from the use of the Goods or any part thereof, or any products produced thereby in association or combination with any other equipment, plant, or materials not supplied by the supplier/ selected bidder, pursuant to the Contract.

b) If any proceedings are brought or any claim is made against the Purchaser arising out of the matters referred to above, the Purchaser shall promptly give the supplier/ selected bidder a notice thereof, and the supplier/ selected bidder may at its own expense and in the Purchaser's name conduct such proceedings or claim and any negotiations for the settlement of any such proceedings or claim.

c) If the supplier/ selected bidder fails to notify the Purchaser within thirty (30) days after receipt of such notice that it intends to conduct any such proceedings or claim, then the Purchaser shall be free to conduct the same on its own behalf.
d) The Purchaser shall, at the supplier's/ selected bidder's request, afford all available assistance to the supplier/ selected bidder in conducting such proceedings or claim, and shall be reimbursed by the supplier/ selected bidder for all reasonable expenses incurred in so doing.
e) The Purchaser shall indemnify and hold harmless the supplier/ selected bidder and its employees, officers, and Subcontractors (if any) from and against any and all suits, actions or administrative proceedings, claims, demands, losses, damages, costs, and expenses of any nature, including attorney's fees and expenses, which the supplier/ selected bidder may suffer as a result of any infringement or alleged infringement of any patent, utility model, registered design, trademark, copyright, or other intellectual property right registered or otherwise existing at the date of the Contract arising out of or in connection with any design, data, drawing, specification, or other documents or materials provided or designed by or on behalf of the Purchaser.

37) **Limitation of Liability**

Except in cases of gross negligence or wilful misconduct: -

a) neither party shall be liable to the other party for any indirect or consequential loss or damage, loss of use, loss of production, or loss of profits or interest costs, provided that this exclusion shall not apply to any obligation of the supplier/ selected bidder to pay liquidated damages to the Purchaser; and
b) the aggregate liability of the supplier/ selected bidder to the Purchaser, whether under the Contract, in tort, or otherwise, shall not exceed the diminishing value of remaining contract, provided that this limitation shall not apply to the cost of repairing or replacing defective equipment, or to any obligation of the supplier/ selected bidder to indemnify the Purchaser with respect to patent infringement.

38) **Force Majeure**

a) The Supplier shall not be liable for forfeiture of its Performance Security, liquidated damages, or termination for default and to the extent that its delay in performance or other failure to perform its obligations under the Contract if the result is of an event of Force Majeure.
b) For purposes of this Clause—Force Majeur means an event or situation beyond the control of the Supplier that is not foreseeable, is unavoidable, and its origin is not due to negligence or lack of care on the part of the Supplier. Such events may include, but not be limited to, acts of the Purchaser in its sovereign capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions, and freight embargoes.
c) If a Force Majeure situation arises, the Supplier shall promptly notify the Purchaser in writing of such condition and the cause thereof. Unless otherwise directed by the Purchaser in writing, the Supplier shall continue to perform its obligations under the

Contract as far as is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

d) If the performance in whole or part or any obligation under the contract is prevented or delayed by any reason of Force Majeure for a period exceeding 60 days, either party at its option may terminate the contract without any financial repercussion on either side.

e) In case a Force Majeure situation occurs with the RISL, the RISL may take the case with the supplier/ selected bidder on similar lines.

39) **Change Orders and Contract Amendments**

a) The Purchaser may at any time order the supplier/ selected bidder through Notice in accordance with clause "Notices" above, to make changes within the general scope of the Contract in any one or more of the following: -

i. drawings, designs, or specifications, where Goods to be furnished under the Contract are to be specifically manufactured for the Purchaser;

ii. the method of shipment or packing;

iii. the place of delivery; and

iv. the related services to be provided by the supplier/ selected bidder.

b) If any such change causes an increase or decrease in the cost of, or the time required for, the supplier's/ selected bidder's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Price or in the Delivery and Completion Schedule, or both, and the Contract shall accordingly should be amended. Any claims by the supplier/ selected bidder for adjustment under this clause must be asserted within thirty (30) days from the date of the supplier's/ selected bidder's receipt of the Purchaser's change order.

c) Prices to be charged by the supplier/ selected bidder for any related services that might be needed but which were not included in the Contract shall be agreed upon in advance by the parties and shall not exceed the prevailing rates charged to other parties by the supplier/ selected bidder for similar services.

40) **Termination**

a) Termination for Default -

The Procuring Entity, without prejudice to any other remedy under the provisions of the Act, the Rules or for breach of Contract, by Notice of default giving two weeks' time to the Supplier, may terminate the Contract in whole or in part

I. If the supplier/ selected bidder fails to deliver any or all quantities of the service within the time period specified in the contract, or any extension thereof granted by PE; or

II. If the supplier/ selected bidder fails to perform any other obligation under the contract within the specified period of delivery of service or any extension granted thereof; or

III. If the supplier/ selected bidder/authorised partner, in the judgement of the Purchaser, is found to be engaged in corrupt, fraudulent, collusive, or coercive practices in competing for or in executing the contract.

IV. If the supplier/ selected bidder commits breach of any condition of the contract.

If Procuring Entity terminates the contract in whole or in part, amount of PSD may be forfeited. In the event the Procuring Entity terminates the Contract in whole or in part, by Termination for Default, the Procuring Entity may procure, upon such terms and in such manner as it deems appropriate, the Goods , Services and Works similar to those undelivered or not performed, and the Supplier shall be liable to the Procuring Entity for any additional costs for such Goods, Works or Related Services and such additional cost shall be recovered from the dues of the Supplier with the Procuring Entity.

b) Termination for Insolvency

PE may at any time terminate the Contract by giving a written notice of at least 30 days to the supplier/ selected bidder, if the supplier/ selected bidder becomes bankrupt or otherwise insolvent. In such event, termination will be without compensation to the supplier/ selected bidder, provided that such termination will not prejudice or affect any right of action or remedy that has accrued or will accrue thereafter to PE .

c) Termination for Convenience

I. The Contract may terminate , in whole or in part, at any time for its convenience. The Notice of termination shall specify that termination is for the Purchaser's convenience, the extent to which performance of the supplier/ selected bidder under the Contract is terminated and the date upon which such termination becomes effective.

II. Depending on merits of the case the supplier/ selected bidder may be appropriately compensated on mutually agreed terms for the loss incurred by the contract if any due to such termination.

III. The Goods that are complete and ready for shipment within twenty-eight (28) days after the supplier's/ selected bidder's receipt of the Notice of termination shall be accepted by the Purchaser at the Contract terms and prices. For the remaining Goods, the Purchaser may elect:- a.To have any portion completed and delivered at the Contract terms and prices; and/or

To cancel the remainder and pay to the supplier/ selected bidder an agreed amount for partially completed Goods and Related Services and for materials and parts previously procured by the supplier/ selected bidder.

41) **Verification of Eligibility Documents by RISL**

RISL reserves the right to verify all statements, information and documents submitted by the bidder in response to tender document. The bidder shall, when so required by RISL, make available all such information, evidence and documents as may be necessary for such verification. Any such verification or lack of verification by RISL shall not relieve the bidder of its obligations or liabilities hereunder nor will it affect any rights of RISL thereunder. If any statement, information and document submitted by the bidder is found to be false, manipulated or forged during verification process, strict action shall be taken as per RTPP Act 2012.

42) **Restrictions on procurement from a bidder of a country which shares a land border with India**

Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered either with the Competent Authority of GoI by Department of Promotion of Industries and internal trade under the Ministry of Commerce and Industry or with the Competent Authority of GoR.

7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT

1) Payment Terms and Schedule

a) Payment schedule - Payments to the bidder, after successful completion of the target milestones (including specified project deliverables), would be made as under: -

S. No.	Milestone/ Phase	Deliverables	Timelines (T= Date of WO)	Payable Amount
Payment Timeline				
1.	Completion of Activities applicable and as mentioned in section 4. (1) (A)	• Delivery Challans "Proof of Delivery" in original.	T1=T+90 days	30% of the total Quoted/Agreed amount in the BOQ-1 of delivered items as per section 4. (1) (after deducting LD, if any and as applicable)
2.	Completion of Activities applicable and as mentioned in section 4. (1) (B)	• Installation Report • OEM Warranty Certificates • OEMs certification of the deployment being in accordance with the scope of work. • Request for UAT along with Test cases report. • Support Escalation matrix document. • Installation, configuration & Integration Document • CV + Relevant Qualification & Experience Documents of Deployed resources	T2=T1+60	NA
3.	Completion of Activities applicable and as mentioned in section 4. (2)	• Request for UAT along with Test cases report.	T3=T2+30 days	40% of the remaining amount of delivered items as per BOQ-1 as per section 4. (1) (A) + 70% of the amount Quoted/Agreed amount in the BOQ-1 for "***Incident Response***

				Solution/Services" and ***"Unified Threat Intelligence Platform (UIP)"*** (after deducting LD, if any and as applicable)
4.	Completion of Activities applicable and as mentioned in section 4. (4) On Quarterly Basis	• SLA Report along with Manpower SLA as defined later in this chapter. • Updated SOP and Rule Review Report • Satisfactory report from the OIC/ designated official at the end of each quarter	Post completion date of respective O&M quarter	Equated in Quarterly i.e., Total Quoted/Agreed in BoQ-2 (Manpower BoQ) /12 Quarters (after deducting penalties, if any and as applicable) + Remaining BoQ-1 payment equated in 12 Quarters i.e. 2.5% of quoted/agreed amount of BoQ-1 at the end of every quarter.

T= date of work order.

b) The supplier's/ selected bidder's request for payment shall be made to the purchaser in writing, accompanied by invoices describing, as appropriate, the goods delivered and related services performed, and by the required documents submitted pursuant to general conditions of the contract and upon fulfilment of all the obligations stipulated in the Contract.

c) Due payments shall be made promptly by the purchaser, generally within sixty (60) days or as early as possible after submission of an invoice or request for payment by the supplier/ selected bidder, and the purchaser has accepted it.

d) The currency or currencies in which payments shall be made to the supplier/ selected bidder under this Contract shall be Indian Rupees (INR) only.

e) All remittance charges will be borne by the supplier/ selected bidder.

f) In case of disputed items, the disputed amount shall be withheld and will be paid only after settlement of the dispute.

g) Payment in case of those goods which need testing shall be made only when such tests have been carried out, test results received conforming to the prescribed specification.

h) Any penalties/ liquidated damages, as applicable, for delay and non-performance, as mentioned in this bidding document, will be deducted from the payments for the respective milestones.

i) Taxes, as applicable, will be deducted/ paid, as per the prevalent rules and regulations.

j) This is selected bidders responsibility to deploy the requisite manpower as per the qualification and experience as define in this bid document. Deployment of unqualified manpower i.e. any manpower who doesn't have the requisite qualification and experience as per this bid document for their respective profile, shall be trated as undeployed/absent manpower and penalties shall be applicable accordingly.

2) Service Level Standards/ Requirements/ Agreement

a) Service level plays an important role in defining the Quality of Services (QoS). The prime objective of service levels is to ensure high quality of services from selected bidder, in an efficient manner to the identified users under this procurement.

b) The service level shall be tracked on a periodic basis and have penalty clauses on non-adherence to any of them. The Bidder shall submit reports on all the service levels to the Purchaser in accordance with the specified formats and reporting periods and provide clarification, if required. The service levels defined below provide for target level of services required, measurements thereof and associated penalties.

c)

#	Service Level Category	Description	Penalty
1	System Availability (Each solution)- Uptime percentage is calculated on a monthly basis for the solutions. In the event of any hardware issues, the Bidder must guarantee the availability of replacement devices to meet the SLAs.	Uptime of 99.5 % and below	1% of the quarterly payable amount towards OPEX of every 0.1% decrease of system uptime.
2	SOC Monitoring- Continuous 24/7/365 monitoring of security events generated from all in-scope devices. Security events will be categorized into Critical, High, Medium, and Low priority. Security events categorization will be carried out collaboratively in consultation with the selected bidder	Critical events should be notified within 30 minutes of the event identification and resolution within 2 hour. Updates should be provided over email at intervals of every 30 minutes or as per the RISL's preferences, as mutually agreed upon with the bidder, until the incident closure. Penalty for missing will be as follows:	100% compliance **i** 1-3 events: 3% **ii** 4-6 events: 5% **iii** 7-10 events: 7% **iv** 11 and above events: 10% of the quarterly payable amount towards OPEX
		High priority events should be notified within 1 hour of the event identification and resolution within 6 hours. Updates should be provided over email at intervals of every 1 hour or as per the RISL's preferences, as mutually agreed upon with the bidder, until the incident closure. Penalty for missing will be as follows:	100% compliance **i** 1-3 events: 2% **ii** 4-6 events: 4% **iii** 7-10 events: 6% **iv** 11 and above events: 10% of the quarterly payable amount towards OPEX
		Medium priority events should be	95% compliance

		notified within 4 hours of the event identification and resolution within 2 business days. Updates should be provided over email at intervals of every 4 hours or as per the RISL's preferences, as mutually agreed upon with the bidder, until the incident closure. Penalty for missing will be as follows:	**i** 1-3 events: 1% **ii** 4-6 events: 2% **iii** 7-10 events: 3% **iv** 11 and above events: 5% of the quarterly payable amount towards OPEX
		Low priority events should be notified within 12 hours of the event identification and resolution within 5 business days. Updates should be provided over email at intervals of every 8 hours or as per the RISL's preferences, as mutually agreed upon with the bidder, until the incident closure. Penalty for missing will be as follows:	92% compliance **i** 1-3 events: 0.5% **ii** 4-6 events: 1% **iii** 7-10 events: 2% **iv** 11 and above events: 3% of the quarterly payable amount towards OPEX
3	Health Check-up observations closure	Unable to close Health Check-up observations within 2 weeks.	A penalty of 1% per week of the quarterly payable amount towards OPEX for non- compliance after the timelines.
4	SOC solution management- Version/ Release / Upgrades / Patches	The bidder should notify the RISL team and guarantee that the entire SOC stack, including firmware, software, middleware, etc., are kept up to date with the latest firmware, patches, upgrades, releases, versions, etc.,	If the patches/signature files are not deployed within a period of 20 working days of RISL from the release of latest version/update by OEM, it will attract a penalty of 0.5% of the charges to be paid for the quarter for the on-site support & remote monitoring services for each week of delay or part thereof.
5	Ongoing Operational Enhancement and Reporting Requirements	The Bidder is required to continuously enhance operations, providing RISL with quarterly or semiannual Gap Analysis reports outlining new improvements, action plans, and their respective progress, which may	Achieve a 2% reduction in event response time on a quarterly basis.

		encompass fine-tuning rules, process adjustments, training for enhanced efficiency and SLA performance, and the introduction of new correlation rules to identify threat patterns, among other areas.	Achieve a 5% reduction in the reporting timeline for critical and high priority events on a quarterly basis. A 2% penalty will be imposed for failure to reduce false positives and for not fine-tuning policies, rules, and correlation rules.
6	Deployed Resource/ Manpower Absenteeism	Availability of the minimum required workforce as per this RFP, with adjustments and additions as mutually agreed upon over time.	1.5* Per day payable amount to the Deployed Resource/ Manpower as per quoted cost for any non-compliance.
7	SOAR Playbook	Achieve a playbook success rate of no less than 95%.	A penalty of 3% of the quarterly payable amount towards OPEX on not achieving the success rate.

*The replacement of a resource by the selected bidder after deployment shall generally not be allowed. However, replacement will be allowed only in case, the resource leaves the organization by submitting resignation with the present employer/ due to poor health condition (supported by certificate issued by a Government Doctor)/ in special cases based on the approval received from the designated authority. If selected bidder change the resource without any stated condition that, penalty of Rs. 50,000/- shall be imposed for every non-authorized replacement. The outgoing resource would complete the knowledge transfer with the replaced resource up to the satisfaction of the purchaser.

In case the supplier fails to rectify the defect(s) in supplied solution within 7 calendar days, it may be considered as breach of contract. Further, in case the fault is not resolved within 24 hours or lodging the complaint three times in a year, it may be considered as breach of contract.

Exclusions from downtime calculation include the following:

- Downtime because of LAN cabling faults.
- Scheduled downtimes (which are approved by risl) on account of preventive maintenance, system testing, system upgrades etc.
- All failures due to source power unavailability and power conditioning, UPS failure etc. beyond control of Vendor Managed Services.
- Force Majeure conditions defined above, or any condition not foreseen but mutually agreed by both the parties.

- Link outages owing to ISPs.
- Downtime due to any device/appliance not managed by the Vendor.

Penalty caps:

- The maximum amount of liquidated damages shall be 10%. The percentage refers to the payment due for associated milestone.
- The total penalty for OPEX shall not exceed 10% of the quarterly charges payable for towards OPEX for reasons other than absence of manpower.

Note: LD/Penalty will not be applicable if there is a delay due to issues pertaining to RISL or reasons attributable to Force Majeure.

3) Change Requests/ Management

a) An institutional mechanism will be set up for taking decisions regarding requests for changes. The Purchase Committee will set up a Change Control Committee with members from the procurement agency and the selected bidder/authorised partner. If it is unable to reach an agreement, the decision of the Purchase Committee will be final.

b) RISL may at any time, by a written order given to the bidder/authorised partner, make changes within the general scope of the Agreement in any one or more of the following: -

- Designs, specifications, requirements which software or service to be provided under the Agreement are to be specifically developed and rendered for RISL.
- The method of deployment, shipping or packing.
- Schedule for Installation Acceptance.
- The place of delivery and/or the services to be provided by the bidder/authorised partner.

c) The change request/ management procedure will follow the following steps: -

- Identification and documentation of the need for the change - The information related to initiator, initiation date and details of change required and priority of the change will be documented by RISL.
- Analysis and evaluation of the Change Request - Impact of the change in terms of the estimated effort, changed schedule, cost and the items impacted will be analysed and documented by the bidder/authorised partner.
- Approval or disapproval of the change request – RISL will approve or disapprove the change requested including the additional payments for software development, quoted man-month rate shall be used for cost estimation, efforts of all technical resources- project manager, analyst, software developer, testing engineer, database architecture etc. shall be taken into account for total man-month estimation to carry out the s/w development resulting from the change request. For all technical resources irrespective of their experience and specialisation, the quoted man-month rate shall be used. Efforts of support staff shall not be taken into consideration for this purpose.
- Implementation of the change – The change will be implemented in accordance to the agreed cost, effort, and schedule by the selected bidder.

- Verification of the change - The change will be verified by RISL on implementation of the change request.

d) All changes outside the scope of supplies agreed to herein which may have likely financial implications in terms of the overall cost/ time of the project shall be undertaken by bidder only after securing the express consent of RISL. In the event that the consent of RISL is not received then the change will not be carried out.

e) While approving any change request, if required, RISL may ask Bidder to deploy the required resources on-site.

f) If any such change outside the scope of supplies agreed to herein causes an increase or decrease in cost of, or the time required for, firm's performance of any provisions under the Agreement, equitable adjustments shall be made in the Agreement Price or Delivery Schedule, or both, and the Agreement shall accordingly be amended. Any claims by firm for adjustment under this must be asserted within 30 (thirty) days from the date of SI receiving the RISL change order which shall not be unreasonably withheld or delayed.

ANNEXURE-1: BILL OF MATERIAL (BoM)

A. Description of Items Required (CAPEX):

S. No.	Item	Qty required at BSDC Jaipur	Qty required at DR-Jodhpur	MAF required (Y/N)	Compliance (Yes/No)
1.	Security Orchestration, Automation & Response (SOAR) Solution with Threat Intelligence Platform (TIP)	1 Nos.	NA	Y	
2.	Incident Response Solution/Services	1 Nos.	NA	Y	
3.	Unified Threat Intelligence Platform (UIP)	1 Nos.	NA	Y	
4.	Network Behavior Anomaly Detection (NBAD)/NDR	1 Nos.	NA	Y	
5.	DNS Security solution	1 Nos.	NA	Y	
6.	Anti-Advanced Persistent Threats solution (APT)	1 Nos.	1 Nos.	Y	
7.	A. SIEM with UEBA	1 Nos	NA	Y	
	B. Network forensic (Packet Capture and Re-Construction Capability)	2 Nos.	1 Nos.	Y	
8.	A. WAF with API Security	1 Nos.	1 Nos.	Y	
	B. DAM	1 Nos.	NA	Y	

B. Technical Manpower (OPEX)

SN	Type of Resources	Qty.	Man month	Total Man month	MAF required (Y/N)	Compliance (Yes/No)
1.	Analyst (Tier-1): 12 Resources x 36 Months	12	36	432	NA	NA
2.	Analyst (Tier-2): 6 Resources x 36 Months	6	36	216	NA	NA
3.	Analyst (Tier-3): 3 Resources x 36 Months	3	36	108	NA	NA
4.	Threat Hunter Regular Day Shift : 2 Resources x 36 Months	2	36	72	NA	NA
5.	Risk & Compliance Auditor - Regular Day Shift : 1 Resources x 36 Months	1	36	36	NA	NA
6.	Forensic Analyst Regular Day Shift: 1 Resources x 36 Months	1	36	36	NA	NA
7.	SOC Manager Regular Day Shift: 1 Resources x 36 Months	1	36	36	NA	NA

8.	OEM Certified Resources - SIEM Regular Day Shift: 1 Resources x 36 Months	1	36	36	NA	NA
9.	OEM Certified Resources - SOAR Regular Day Shift: 1 Resources x 36 Months	1	36	36	NA	NA
10.	OEM Certified Resources -WAF Regular Day Shift: 1 Resources x 36 Months	1	36	36	NA	NA
11.	OEM Certified Resources – NBAD / Network Forensic Regular Day Shift: 1 Resources x 36 Months	1	36	36	NA	NA

Note: -

a. All the OEM's of products at Si No:1,3,4,5,6,7,8 of Table-A, should be distinct. It is to be ensured that the MAFs submitted for each product clearly identify the distinct OEMs.

b. All the required accessoris required for installation need to be supply by selected bidder.

c. For all items mentioned in annexure-1 shall be provided with Onsite/Remote Comprehensive OEM warrenty and premium support (24*7) form the date of commissioning / Go-live for 3 years

d. All hardware / software would be (on-premise) in nature having perpetual license. If any OEM doesn't provide perpetual license (as per their policy) for the respective software than only subscription may be considered and the bidder has to submit the relevent evidence in the technical bid.

e. Licenses shall be in the name of *'Department of Information Technology and Communications, Government of Rajasthan'*.

f. All the OEM's of products at Si No:1,4,5,6,7,8 of Table-A, must supplied with the training license i.e. an additional license for 1 quantity if the offering is virtual. For a hardware offering, choose the lowest module of the device that meets all the features listed in the product specifications. This would be used in Cyber-Range platform (OEM: Keysight, CySOP platform) for Training Purpose.

g. All the quoted H/w and S/w components must be IPv6 ready from day one and should be supplied with 3 Years comprehensive OEM on-site warranty and services from the Go-Live Date. This means that in case calls are lodged to OEM (through SI or purchaser) for support-services-guidance, OEM shall ensure comprehensive onsite/remote OEM support and services.

h. The deployed manpower should be on bidder's permanent payroll.

i. To ensure required Minimum Level of Resource quality, following floor limit for Resource Cost to be quoted / factored –

- L1 Resource – Rs. 7.5 LPA with minimum year increment of 7 to 8 %.
- L2 Resource - Rs. 9.5 LPA with minimum year increment of 7 to 8 %.
- L3 Resource - Rs. 14 LPA with minimum year increment of 7 to 8 %.
- SOC Manager - Min. 20+ LPA with minimum year increment of 7 to 8 %.

Note: The minimum compensation for the resources shall be at least as per the above figures. RISL reserves the right to verify the same.

j. RISL will conduct interviews and/or assessments utilizing the Cyber Range platform to evaluate the suitability of proposed resources for R-SOC. RISL reserves the right to reject any resource deemed unsuitable for the intended role.

k. Detailed technical specification of the equiment in Annexure-1 are the minimum requirments and bidders may quote/supply equipment with higher specifications although purchaser shall not pay for any higher specification

l. Shift Detail

- **a.** Shift 1: 6AM – 2PM
- **b.** Shift 2: 2PM – 10PM
- **c.** Shift 3: 10PM – 6AM
- **d.** Regular Day Shift: 9:30AM – 6PM

Name of the Bidder: -
Authorised Signatory: -
Seal of the Organization: -
Date: _____
Place: _____

ANNEXURE-2: TECHNICAL SPECIFICATION

Item No. 1: Security Orchestration, Automation & Response ( ) Solution with Threat Intelligence Platform (TIP)

Make & Model offered:…… (need to be filled by the bidder)

Sr. No.	Minimum Feature Requirements	OEM Compliance (Yes/No)
	Basic Features	
1.	The proposed solution should be a fully on premise solution deployed in-house with all the capabilities of Security Orchestration & Automation (SOA), Security Incident Response Platform (SIRP) and Threat Intel Platform (TIP) as part of single or multiple licenses. Bidder should ensure all the necessary proposed SOAR solution must have native integration with proposed SIEM platform.	
2.	Solution Should have documentation readily available for using automation.	
3.	Solution should support standard languages like Python, JS & Powershell to create and customize scripts including CI/CD pipeline.	
4.	Solution should support integration with following technologies. • Forensic tools, specify all products. • IT (e.g., AD, SAML) • Communication tools (e.g., email, Slack) • SIEM tools • Endpoint Security Solution • Network Security Solution • Web Proxy • Threat Intelligence • Dynamic malware analysis	
5.	Solution should support adding of new product integrations.	
6.	The proposed solution should have min 650+ built-in out of the box reusable playbooks for well-known incident types (Phishing, Malware, IOC Hunt etc.) from day one without any restriction in creating number of playbooks i.e. out of box and customized playbooks and re-use of playbooks in bigger playbooks in the provisioned license. Solution should support addition of automation scripts to existing integration Playbooks.	
7.	The SOAR solution should support 600+ integrations out of the box.	
8.	Integration packs should include pre-built use cases consisting of	

	playbooks, automation actions, scripts that can be customized	
9.	The solution should have an integration store that is continuously updated with both OEM and Partner provided integration.	
	Playbooks	
10.	Solution should use playbooks.	
11.	Solution should have built in playbooks.	
12.	Solution should allow creating new playbooks.	
13.	Solution should support re-use playbooks in bigger playbooks.	
14.	Solution Should allow creation of Manual Tasks, Automated Tasks and Conditional Tasks in Playbooks	
15.	Solution should allow a single playbook to have Automated and Manual Tasks	
16.	Solution should allow a complete playbook to be run automatically and should list out any exception.	
17.	Solution should allow a complete playbook to be run manually and should list out any exception.	
18.	Solution should record all manual and automated entries during execution of a playbook.	
19.	Solution should allow addition of ad-hoc tasks in a playbook.	
20.	Solution should support scheduled tasks.	
	Incident Management	
21.	Solution should integrate with Incident management tools	
22.	Solution should provide an incident management platform for Security and IR team	
23.	Solution should support assigning of incident to a User or a group	
24.	Solution should maintain SLA for incident	
25.	Solution should identify and differentiate incidents from all states	
26.	Solution should support sending notifications to other users	
27.	Solution should specify the mode of receiving an incident for example (REST API, mails, Syslog etc)	
	Documentation	
28.	Solution should document all artifacts related to an incident	
29.	Solution should provide documentation on process for documentation of evidence	
30.	Solution should record timestamp for all actions taken in an incident	
31.	Solution should document all manual tasks perform by user in an incident	
	Collaboration	
32.	Solutions should allow users to collaborate within the platform	
33.	Solutions should have filters in place to quickly identify relevant investigation data from the virtual war room	
34.	Solution should support external users to contribute to an incident	

35.	Solution should highlight is any external products are required for Collaboration. It should provide an exhaustive list of such products currently supported	
36.	Solution should have an integrated chatops BOT functionality which can help in collaboration and automated response.	
	Architecture	
37.	The solution should support High Availability (Active-Passive or Active-Active cluster) natively without using third party solutions. All necessary Hardware & software for the proposed solution to be provision by the bidder as part of solution from day 1	
38.	Solution should be deployed on a containerized platform and every playbook execution/integration should be inside a container to minimize the risk of lateral movement compromise in case of supply chain risk introduced by an integration.	
39.	Solution should support multitenancy and provide a clear Architecture for function in multi-tenant environment	
40.	Solution should support multiple modes(SSH, API etc.) to access supported remote devices.	
41.	Solution should list out any agents used by it and the supported platforms/OS	
42.	Solution should support searching of Data/artifacts associated with historical incidents Administration	
	Administration	
43.	Solution should support backup / restore	
44.	Solution should provide predefined reports	
45.	Solution should support creation of customized reports	
46.	Solution should provide out-of-the-box shift management	
47.	Solution must have an authenticated API capable of executing the same functions as are available via the GUI	
48.	Solution should have strict RBAC to govern the usability and accessibility of the platform. Solution should have RBAC for dashboards	
49.	Solution should support Dashboard and any Dashboard which can be provide high level view of Platforms KPI's to the management	
50.	Solution should support upgrading features and provide relevant documentation for upgrading itself	
51.	Solution should allow for viewing version history for all or selected playbook and provide option for restoring to an older version	
52.	Solution should support updates for Playbooks, Integrations and should specify the procedure to update each of them	
53.	Solution should support SAML 2.0 and 2 Factor Authentication, also provide an list of Authentication options available	

	Others	
54.	Solution should have a documented Information Security Management (ISM) program and adhere to security standards such as ISO27001	
55.	Provided solution should support at least 10 concurrent analysts.	
56.	Solution should be able to integrate with at least 2000 devices from day one	
57.	SOAR solution (Engine / OS / hardware) should be certified under Common Criteria (global or the Indian Common Criteria Certification Scheme(IC3S) has been set up by the Ministry of Electronics and Information Technology (MeitY)) program.	
58.	The OEM of the proposed solution should be present in Leaders in Giagaom Radar Report for Autonomous Security Operations Center (SOC) in any of last two reports	
Threat Intel Platform (TIP)		
59.	Centralized platform should provide real-time threat feeds of proposed OEM including automation of collection and aggregation of threat intelligence data. Solution should be on-prem and part of SOAR	
60.	Platform should automate entire intelligence lifecycle, proactive threat monitoring and accelerate incident detection and response	
61.	Platform should automate, streamline and simplify the entire process of researching, collecting, aggregating and organizing threat intelligence data, as well as normalizing, de-duping and enriching that data.	
62.	TI feed should be refreshed on TI Platform immediately on any new threat identification or any new attack observed around globe.	
63.	The threat intelligence platform must use machine learning to harvests and structures text content from sources across events, enabling analysts to perform powerful and intuitive searches that go beyond bare keywords and simple correlation rules	
64.	The collected intelligence should have at least 10 years of historical data and should be included in query results on Portal with event details	
65.	The platform should provide IOC with reliability score, detection quality or risk score. Scores must be justified with rational behind the given scores. Scores must be dynamic to represent the automated real-time risk of the said IOC.	
66.	The platform shall be able to provide the ability to contextually link reported security events with real time knowledge of the assets that are being targeted.	
67.	The threat intelligence platform must be able to collect and integrate	

	data feed from GOI agencies like NCIIPC, Meity, CERT-In and other certified government agencies	
68.	The threat intelligence platform must allow users to request data review or validation of threat intelligence	
69.	The platform should be able to provide the vulnerabilities being exploited by the threat actors actively with sources as such Vulnerability Assessment Tools, Threat feeds, etc. TIP should have a dedicated Vulnerability Management Module.	
70.	The threat intelligence solution must enable end users to identify references to critical zero-day exploits based on threat intel , etc.	
71.	The platform should support integration with existing / proposed SOC tools, vulnerability management tools such as SIEM, SOAR, Deep Analysis tools, TIP, EDR, Firewalls, UEBA, DNS Proxy and other devices to integrate the feeds.	
72.	The platform should support to ingest data from multiple formats such as STIX/TAXII, JSON, XML, PDF, CSV, email for analysis.	
73.	The platform should be able to provide alerts via Portal, Email etc. which can be worked upon by RISL's team.	
74.	"The threat intelligence platform must be able to support analysis with: a. Real-time trends and developments b. Historical view of related events c. Reported roles involved in the events (attackers/threat actors, targets/organizations) d. Reported TTPs (attack vectors, malware, exploits) e. Reported indicators (IP addresses, domains, hashes, URLs etc.) f. Related operations g. Access to the original references with cached content for the volatile ones h. Other contextual details about the events"	
75.	Platform should facilitate user to Create monitor, automate alert and report for Vulnerability based Threats but not limited to following a. New critical vulnerability announcement and world risk of the vulnerability at Pre- NVD level b. Trending Vulnerabilities posing security threats to RISL Technology Stack	
76.	Intelligence platform should include provisioning of hunting tools, such as YARA rules, SNORT rules, MITRE ATT&CK Identifiers to assist the RISL to hunt for adversaries,	

	malware, or traffic of interest wherever available	
77.	Platform should also provide context around Vulnerability with real world criticality apart from CVSS score and should be able to integrate with leading vulnerability assessment vendors	
78.	The Threat Intelligence platform integration should be hardware independent- while integrating with multiple threat intelligence sources to provide comprehensive advanced threat protection.	
79.	Bidder should integrate both open-source and commercial intelligence feeds into the platform.	
80.	Proposed TI platform console should have Network Graph Analysis/Native /graphical customizable dashboards feature to search and provide results for any of the IOCs such as Historical data, associated domains, IPs, SSLs etc, The platform should provide dashboards and visual representation in network of insights and findings, which can be downloaded in various formats such as PDF, CSV, etc.	
81.	The solution must have comprehensive set of free OSINT feeds integrated with the platform.	
82.	Solution must ensure that apart from other relevant elements, the following elements are included in the IOC: i. Source information (IP, Domain, URL etc.) ii. File formats (.exe, .doc, .pdf,.xml etc.) iii. Geo Location iv. File hash values v. Vulnerability details	
83.	"Solution should present the imported feeds in a graphical, searchable, sortable and reportable format in the platform itself."	
84.	Solution must provide additional information on IOCs, wherever requested, by integrating with WHOIS, Virustotal, Shodan, Hybrid Analysis etc.	
85.	Solution should be able to provide latest threat advisories in a searchable manner based on geography, threat actors, IoC etc., to obtain the information about Tactics, Techniques, and Procedures (TTPs).	
86.	Solution should be capable of mapping the TTP to APT Groups to zero down the APT groups targeting RISL	
87.	Solution should have the capability to set an expiration for TLP: RED STIX packages for secure transfer and handling of valuable tactical threat information.	

88.	Solution should have capabilities to perform Custom scoring based on parameters like source weightage, source, score, etc.	
89.	Solution should allow sharing and receiving of Technical Threat Intelligence.	
90.	Solution should support sharing real-time enriched and analyzed Threat Intel with peers, subsidiaries, third parties, regulators etc.	
91.	Solutions should be able to trigger automation if an IOC attribute is changed	
92.	Solutions should have whitelist management built-in to reduce false positives	
93.	The platform should have an out-of-the-box Threat Intelligence Playbook library which would help in automating threat intel based use cases such as IOC hunting, IOC Dissemination, IOC to Vulnerability mapping etc.	
94.	The solution should provide a plugin or support open source plugin or allow uploads that can scan web pages, Outlook, Word, Excel, PDF document being viewed for IOCs, including IPs, Domains, URLs and Hashes, Attack pattern and allow the IOCs to be used interactively with the solution.	
95.	The solution must support the ability to detonate any malware attached to, or as a URL embedded in a phishing email, and capture any IOCs generated by the detonation as linked to the email by integrating existing sandbox solution.	
96.	The solution must allow the analyst to extract/import the content for further analysis in an analyst workbench, such as performing link analysis and enriching context from third party sources, before finalizing the import and storing as a threat intelligence product.	

Item No. 2: Incident Response Solution/Services

As a part of solution, Bidder/ OEM shall propose the Incident Response (IR) services from a Global security OEM with more than a decade of incident response experience, which should primarily include: -

- One-time Incident Response Plan development services from OEM after the commencement of SOC including its review/ revision at the beginning of every next year for the duration of contract. Below is a list of the key information that will be available with RISL as part of incident response plan:
  - Contact information for the Incident Response Team and other relevant stakeholders
  - Procedures for reporting security incidents
  - Assignment of roles and responsibilities for the incident response team
  - Escalation paths for serious incidents or unexpected challenges to IR Service Provider
  - Procedures for reporting, documenting and evaluating security incidents
  - Update and review processes to ensure the plan remains current and effective
- Minimum 30 Man Days or 240 hours of OEM IR services per year (for 3 Years) whenever required by RISL.

Sr. No.	Minimum Feature Requirements	OEM Compliance (Y/N)
1.	The OEM must provide full-spectrum Incident Response (IR) services, ensuring rapid response and comprehensive support for the identification, containment, eradication, and recovery from cybersecurity incidents. (240 hours per Year for 3 Years)	
2.	OEM must provide advice/Guide on full scope of cyber security incident response (IR) retainer service including. ▪ Identification ▪ Containment ▪ Eradication and Recovery ▪ Malware analysis and reverse engineering ▪ Reporting ▪ Incident response readiness assessment ▪ Incident response plan development ▪ Cyber Range training ▪ Advanced threat hunting ▪ Cyber security assessment including Network Security Architecture Assessment	
3.	OEM must execute the IR Plan development considering the following: ▪ An IR Plan should foster a continuous improvement process that leverages lessons learned from past incidents to improve overall security effectiveness. ▪ An IR Plan documents the processes and procedures, roles and	

	responsibilities of various stakeholders, and communications flows and notifications procedures that are critical in timely recovery from security incidents. ▪ The IR practice should have a closed loop feedback into the intelligence program.	
4.	OEM must provide following activities as part of Advanced Threat Hunting: ▪ Planning: o Project Planning o Understand requirements and define scope. o Identify available log telemetry sources within customer infrastructure o Leverage End-point Agents o Leverage Network Forensics Platform ▪ Data Capture & Gathering o Perform End-point Sweeps and gather data for analysis. o Perform Full network capture over a defined time interval. o Gather logs and alerts (DNS, Firewall etc.) ▪ Detection & Analysis o Perform network packet analysis. o Use Intel, OSINT and Indicators of Compromise (IOC) to look for attack patterns. o Identify additional IOCs. ▪ Reporting o Detailed Network hunting report o Detailed End-point hunting report o Management Presentation o Recommendations to improve security posture.	
5.	Annual Advanced Threat Hunting service should include provision of necessary tools deployment at BSDC to provide the necessary report to highlight presence (incase presence is there) of compromises and threat activities previously un-identified in customer environment as and when required.	
6.	The services being proposed should be of global cyber security standard and should be in use in any Government/ BFSI/ PSU/ Public limited companies in India. The OEM should have experience in handling and responding to Advanced Persistent Threats (APTs),	
7.	The OEM should have identified new APTs/ Adversaries and published APT/Threat Reports in public domain (samples of latest 5 APT/Threat reports to be submitted along with the Bid).	

	OEM should be publishing, an annual threat report detailing information on adversaries and related attacks on Government/ BFSI/ PSU/ large enterprise and related industries.	
8.	OEM must have SANS certified engineers to undertake proactive Threat hunting. These Engineers must have at least 10 years of industry experience in IR.	
9.	OEM must have produced research papers, published vulnerabilities, and won awards in the industry. OEM should have at least 10 resources Incident Response professionals with average of 10 years in-field active investigation experience.	
10.	OEM must have at least 6 cyber security experts that hold at least 2 of the following security certifications/ qualifications: • Certified Information Systems Security Professional (CISSP) • Certified Incident Handler (GCIH) • Certified Information Systems Auditor (CISA) • Certified Information Security Manager (CISM) • Certified Ethical Hacker (CEH) • GIAC Certified Forensic Analyst (GCFA) • GIAC Certified Forensic Examiner (GCFE) • Certified in Risk and Information Systems Control (CRISC) • Certified Cloud Security Professional (CCSP) • GIAC Cyber Threat Intelligence (GCTI) • CompTIA CySA+ (Cybersecurity Analyst) • Offensive Security Certified Professional (OSCP) • Certified Expert Incident Responder (CEIR) • Incident Handler (E|CIH) • ISO/IEC 27001 Lead Implementer / Lead Auditor • PCI Professional (PCIP) • Certified Threat Intelligence Analyst (CTIA) • GIAC Security Essentials Certification (GSEC) • GIAC Web Application Penetration Tester (GWAPT) • GIAC Cyber Security Professional (CSP) • GIAC Experienced Forensics Analyst (GIAC-GXFA) Note: OEM must submit a declaration on his letter head along with qualification and certifications of such resources.	
11.	The OEM must emulate the tactics, techniques, and procedures (TTPs) of advanced persistent threats (APTs), cybercriminal groups, and other sophisticated attackers.	

	OEM should conduct multi-stage attacks, focusing on reconnaissance, privilege escalation, lateral movement, and data exfiltration exercise to understand the risk and present a report. OEM must use various attack vectors, including spear phishing, social engineering, network exploitation, and system compromise.	
12.	The OEM must simulate targeted attacks based on real-world TTPs derived from intelligence sources. It should provide the RISL with the experience of a sophisticated targeted attack without the damage and costs of a real breach. Solution should provide Ransomware Readiness with would help RISL's to conduct Ransomware readiness & Ransomware Resilience to prevent, detect, and better respond to ransomware attack. OEM to work with RISL for tabletop Exercises to develop a plan to help RISL to improve security posture and execute work according to that plan agreed over the course of the retainer/contract.	
13.	OEM must perform detailed forensic analysis, including disk and memory examination, and provide reports detailing the Indicators of Compromise (IOCs) and attacker behaviors. OEM must provide: • Incident Reports: Detailed post-incident reports, including root cause analysis, attack timelines, and recommendations. • Strategic Recommendations: Strategic remediation recommendations mapped to industry frameworks such as MITRE ATT&CK. Containment and Remediation: The OEM must provide guidance on containment measures and full system remediation procedures.	
14.	The OEM must be listed in the Gartner Market Guide for Digital Forensics and Incident Response Retainer Services and offer Detection and Response services. The OEM must have a track record of achieving more than 32 Detections/100% protection & visibility in MITRE Engenuity ATT&CK Evaluations for Managed Services, as per the 2023 or 2024 report.	

Item No. 3: Unified Threat Intelligence Platform (UIP)

Make & Model offered:…… (need to be filled by the bidder)

Sr. No.	Minimum Feature Requirements	OEM Compliance (Yes/No)
	General Requirement	
1	The Commercial threat feed shall be integrated with the SIEM/TIP Platform using API/REST API.	
2	The Commercial feed integration steps shall be thoroughly documented by the commercial threat feed OEM on their website or support portal/knowledgebase.	
3	The threat feed should also be provided via API/REST API. OEM should provide web-based portal for providing intelligence details on IP Address, Indicators of Compromise (IoCs) etc. for one security analyst from day one.	
4	The provider shall be able to provide extensive context-aware indicators and malware analysis in addition to the threat indicators. Information shall include but not limited to, background of the threat actors and attack methods linked to specific indicators and threat artefacts.	
5	Ensuring the security and, confidentiality of RISLs data in the cloud will be the sole responsibility of the provider. The provider shall ensure that the best practices provided by OEM are implemented in the services provided to RISL	
6	Threat Intel provider must have more than 10 years of threat intelligence collection experience, analysis and tracking across deep web, dark web, OSINT, social media, and other sources. The data should be searchable on the platform with the required sates and time stamps	
	Threat Intel Feed Requirements	
7	The solution must be offered with API/REST API based integration to provide high severity block grade Threat feeds (e.g. risk score > 65 or risk rating very critical, high, etc.) directly into security tools like SIEM, SOAR, TIP platforms etc.	
8	The Threat feeds must be auto updated in near real time or maximum in 24 hours for IP addresses, domains and URLs, hashes and once every week for CVEs.	
9	It shall be possible to check the current risk score/rating or confidence level of any IOC like IP Address, domain, URL, hash etc. with reasons of why an IOC is good or bad. The scoring mechanism shall be made available to RISL to understand why any IOC is risky.	

10	The Threat feeds must be collected from multiple third-party sources both OSINT and paid, it shall be de-duplicated and then offered to RISL for integration.	
11	The provider shall provision adequate professional services from the TI OEM or it's authorized partners for one-time configuration of the TI feeds with RISL SIEM and shall provide 1- day training to RISL team.	
12	Threat intel feeds from the platform shall be integrated with RISL's current SOC solution in STIX, TAXII 2.0 format or via Web API/REST API.	
	OSINT Capabilities	
13	The solution must provide complete intelligence (historical and latest) about entities, proprietary or OSINT sourced, in a single viewing pane with the following minimum information. (i) IP Addresses (ii) Domains (iii) Hashes (iv) URLs (v) Related Malwares/Threat Actors (vi) OEM research reports (vii) Hunting Packages, if any	
14	The portal shall provide for search capability for searching of various IOCs, Threat actors, cyber-attacks, Malware, Industry, Region etc. The portal shall allow change and customization of query logic on the fly from portal for faster and specific analysis and get actionable intelligence.	
15	The threat intelligence portal solution must provide an option to request for Intelligence data review to report incorrect reference, risk scoring/rating etc from the OEM directly from the web portal	
16	The web portal must provide context or co-references with other IOCs. (Eg other IP addresses within the CIDR and their risk scores/rating).	
17	The web portal shall allow download for hunting packages such as YARA rules, MITRE ATT&CK Identifiers to assist in hunting for adversaries, malware, or traffic of interest wherever available. The hunting packages shall be coming from its own Threat Intelligence rather than from third party.	
18	The solution shall provide mappings of TTPs to MITRE ATT&CK framework.	
19	The web portal must offer a Ransomware and Malware Dashboard to understand the trending ransomwares filtered on per country or industry basis.	
20	The web portal shall have the capability to perform ad hoc searches using the quick search box.	
21	The Web portal shall have encrypted access using SSL (https) and must be accessible 24/7 from anywhere.	

22	The web portal shall be provided with Two factor authentication for accessing the WebUI portal. Acceptable 2nd factor is SMS or via mobile application. The 2FA solution shall be provided by OEM/provider.	
23	The web portal shall provide cyber security news on a daily basis via email and web portal and along with its analyzed point of view.	
24	The solution shall facilitate to create, monitor, automate alert and report for Vulnerability based threats on new critical vulnerability announcement and real-world risk of the vulnerability.	
25	The threat intelligence solution must enable RISL team to identify references to critical zero-day exploits (if available) in the portal.	
26	The offered solution must provide information about whether an vulnerability is actively exploited, exploit code is available and any threat actor is associated.	
27	**Deep and Dark Web**	
	The platform shall incorporate a range of multi- layered monitoring services and analysis techniques and correlates data across a range of resources including: Social media Public repos Forums Dedicated leak sites File shares Criminal marketplaces Dark Net blogs, forums	
28	The solution must provide Threat intelligence findings from analysis to “midpoint traffic data” on the internet between threat actors, malicious infrastructure, and customer owned and managed IP address.	
29	Intelligence provided must have reference to the source of information including Dark web and Deep web and Paste bin sites, either through a direct link to the source or a cached copy without the need for Customer to actually going onto Dark web to look for evidence.	
30	The offered solution must have a capability to create a prebuilt or custom dashboard or custom dashboard which provides information on the Threat Actor and Malware, or attribution based on the RISL defined watch lists.	
31	The solution must Monitor Discussions of Malicious actors asking for/selling confidential information or selling breached databases, etc	
32	The provider shall be able to provide the facility to analysis the historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity)	
33	Platform shall provide intelligence from Internet traffic analysis to look for possible exfiltration or C2 extraction from RISL PUBLIC IP range.	
34	The solution should also be able to crawl information from invite only dark web forums	

35	The solution must also crawl multiple anonymous messaging platforms like telegram, discord to detect any threats for the client's brand	
36	The solution must be able to look for Exploit Proof of Concepts on selective technologies & sources like Dark Web and Underground forums to visualize and reduce Zero -day exploits.	
37	The provider shall provide the facility for searching the categorization of the historical data of the threat actor, threat activity, threat objects (historical data of the IPs, URLs, etc. used by the malicious entity) linked on a single view.	
38	The proposed threat intelligence solution shall have an in-built cloud based sandboxing/File Analysis feature, without the need to partner or bundle with third party/external sandboxing vendors, for detonating and analysis of suspicious files with 1000 files/analysis per day.	
39	The sandbox solution must be capable of analyzing files on Windows, Linux, Android and Mac environments.	
40	The sandbox solution must be capable of analyzing full and short URLs, dark web URLs (.onion links) and QR code/ images	
41	The sandbox shall protect organizational privacy by not uploading the file to any publicly accessible repository or third-party portal except on OEM's managed portal.	
42	The solution must display images in the search results from sources such as Twitter, LIVEUAMAP, Ransomware extortion sites such as ALPHV, Arvin Club etc and link it to the current context.	
43	The solution must apply techniques like Image OCR or logo detection/typo squatting to identify fake and fictitious websites and documents being sold on deep and dark web	
44	The solution must offer a facility to create, monitor, automate alert and report and advance threat research for threat on Clear, Deep/Dark Web, Underground and special access forum around the following use cases: a. Intellectual property exposed or leaked b. Mentions about RISL around cyberthreats and threat actors c. Cyber threat trends to peer Industry (Govt state DC infrastructure and state govt entities) d. Credential Leak found e. Direct Threats to RISL f. Brand Mentions on Sensitive Sources g. Infrastructure Targeted or Leaked h. Mentions of IP Addresses and Infrastructure i. Mentions of Business Assets j. Monitor Malicious or Typosquat Domains registrations k. Identify and uncover C2 communications with RISL IP Addresses	

	l. Monitor for Brand mentions in sources Messaging platforms like Telegram, vKontakte, Discord, etc. (if any)	
	Brand Monitoring and Social Media Monitoring	
45	The solution must monitor all major RISL/DoIT domains including but not limited to rajastahn.gov.in and other domains and report and alert about typo squat and non-typo squat domains similar to the given domains handled by Government of Rajasthan. The major domains are around 15-20, sub domains are around 3-4 thousand.	
46	The solution must monitor the domain and subdomains to identify/locate assets, services, security issues, phishing risk associated and misconfigurations across public facing DoIT&C/RISL assets.	
47	The solution should monitor code sharing platforms to ensure propriety code is not leaked.	
48	The solution must cover RISL's unlimited digital assets including but not limited to Watchwords, Domains, VIP executives, WHO-IS and DNS information etc	
49	The solution must support multi language watchwords like Hindi / local Indian Languages	
50	The solution must Identify rogue/ fake mobile apps version of of RISL & DoIT apps on Play store and other similar third party application stores.	
51	The solution must monitor impersonation activities around key VIP executives of RISL and associated entities.	
52	The solution must monitor mentions of the customer digital assets on social media websites and Messaging platforms like Telegram, vKontakte, Discord etc	
53	Solution should be able to flag impersonating profiles across all major social media platforms (Linkedin, X/Twitter)	
54	The solution must report about any Internal/Confidential Document found on websites like Scribd	
55	Identify Imposter applications often leveraging client Intellectual Properties such as logos/OCR image, brand names etc on the both official and Google/iOS/Microsoft	
56	The solution should provide a screenshot of the domains associated with domain abuse alerts and can request an updated image be taken directly from the same page on web portal	
57	The solution must be offered to assist RISL to takedown fake and fictious URLs, websites and sensitive domains. At least 25 takedown per year may be factored with the solution.	
58	The should scan RISL brand continuously and combat fake social media content / discussions happening (e.g., Twitter, LinkedIn etc.) that could	

	harm its brand image and reputation and take all necessary steps for their takedowns	
	Attack Surface Monitoring	
59	ASI/ASM shall provide an outside-in view of RISL, enabling to see the blind spots that are visible to adversaries and move the advantage back to RISL.	
60	ASI/ASM shall provide RISL with a complete understanding of their attack surface via a real-time snapshot of all on-premise and cloud- based assets on the internet at any given time.	
61	The solution must scan unlimited number of RISL provided domains and sub-domains on continuous basis with no restriction on the number of sub-domains or number of hosts being scanned.	
62	The solution shall offer a complete inventory of internet facing assets of RISL spread across various domains, total hosts name count within each domain., total active hosts and total inactive hosts. The tool shall provide an option to download the inventory information and the risk results in CSV/excel friendly file formats.	
63	The solution shall be able to monitor and identify: - popular open ports on the hosts such as RDP, HTTP, HTTPS, SMTP, DNS, POP3, POP3S, SMTP, IMAP, IMAPS, TELNET, FTP etc. - open database ports such as PostgreSQL, ElasticSearch, MySQL, MS-SQL, MONGODB etc. - hosts with self-signed certificates - recently discovered hosts.	
64	The solution must be able to scan and identify the following misconfigurations and vulnerabilities on internet facing assets of RISL: - Remote Code Execution vulnerabilities - XSS Vulnerabilities - Server Information Disclosure - Open RDP instances - Applications with Default and Unauthenticated Access - Exposed Services such as PhpMyAdmin, DB Instances, - - Apache Tomcat managers etc. - Vulnerable versions of software - Default application logins	
	Leaked Credential	
65	The solution must provide the following details in respect of a leaked credentials for a given authorized organizational domain for the following: - Leaked Username or Leaked Email Address - Full unsalted hashes in encrypted format (eg SHA1, MD5, SHA256, NTLM) - Clear text password hint (first 2 characters) or full cleartext password to	

	enable credential owner to identify and remediate their use of the exposed password. - Details on applications URL for which the credential works - Type of exposure (clear password or hash type) - Session Cookie Details - Password Properties of the leaked credential	
66	The solution shall provide information about the leaked credential events such as first and last downloaded date, compromise date linked to these dumps (zero or more.) wherever available.	
67	The solution must provide relevant dashboards to highlight credential exposure and details like top domains, technologies, dominant malware etc.	
68	The solution must offer summarized alerts to identify novel credential exposure.	
69	The solution must have option to restrict view of cleartext password for limited admin users only or have a role to have read only role.	
	Support and Training	
70	The solution must be provided with 24/7 access to the support team via web, email and phone. The solution must include support from OEM for continuous product usage support and regular reviews.	
71	The solution shall include on-boarding training for 10 analysts.	
72	The OEM of the solution must provide access to unlimited online training to the offered solution.	
73	The solution must include one remote intelligence analyst from OEM for continuous product usage support and regular reviews.	

Item No. 4: Network Behavior Anomaly Detection (NBAD)/NDR

Make & Model offered:…… (need to be filled by the bidder)

S. No.	Minimum Feature Requirements	OEM Compliance (Yes/No)
1.	The solution must be deployed on premise.	
2.	Should have an automated discovery function to identify network devices and capture information such as IP address, OS, services provided, other connected hosts.	
3.	Should have minimum 175,000 fps / 25 Gbps from day one.	
4.	The solution must support hundreds of ML models for enhanced detection and should not rely only on Rules/IOCs for threat identification.	
5.	Should Identify the source of an attack and should not block legitimate users.	
6.	Should identify worms through techniques such as identifying the use of normally inactive ports or identification of network scanning activities.	
7.	The solution should be capable of detecting denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks including floods of all types (ICMP, UDP, TCP SYN, TCP NULL, IP NULL etc.), identify the presence of botnets in the network, identify DNS spoofing attack etc.	
8.	Should be capable of conducting protocol analysis to detect tunneled protocols, backdoors, the use of forbidden application protocols etc.	
9.	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.	
10.	Should support the capability to instruct network security devices such as firewalls to block certain types of traffic or route it to quarantine VLANS.	
11.	The system should be able to monitor flow data / Packet data between various VLANS.	
12.	Should support the capability to identify network traffic from high-risk applications such as file sharing, peer-to-peer, etc.	
13.	Should support the capability to link usernames to IP addresses for suspected security events.	

14.	Should support the capability to extract user defined fields (including source and destination IPs, source and destination MAC address, TCP/UDP ports or ICMP types and codes, no. of packets and no. of bytes transmitted in a session, timestamps for start and end of session etc.) from captured packet data and then utilize fields in correlation rules.	
15.	Should support the capability Application profiling in the system and should also support custom applications present or acquired by the customer.	
16.	Solution should be compatible with a virtual environment.	
17.	Dashboard should have the facility to be configured according to user profile.	
18.	System should support event forwarding for SMTP, SYSLOG & SNMP for high-risk issues.	
19.	The solution must allow analysis by grouping of network segments such as User VLAN, Management VLAN, Server Farms etc.	
20.	Solution should be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.	
21.	Solution should support ubiquitous access to view all reporting functions using an internet browser.	
22.	The solution should support the identification of applications tunneling on other ports.	
23.	Solution should be able to collect security and network information of servers and clients without the usage of agents.	
24	The solution should support all forms of Packet/ flows including but not limited to netflow, jflow, sflow, ipfix for udp etc.	
25.	Solution should provide the internal network visibility and actionable insight required to Quickly identify and troubleshoot a wide variety of network issues. Additionally, solution integrates user information with network traffic statistics to deliver detailed intelligence into user activity anywhere across the network.	
26.	Solution should also collect and analyze device through integration with the NAC (Network Access Control) devices.	
27.	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.	
28.	Solution should detect the various steps of advanced attacks including: • Network Reconnaissance • Internal Pivoting • 0-day Malware	

	• Botnet (C&C) Communications • Data Exfiltration	
29.	Solution must detect the full spectrum of worms, viruses and botnets, including 0-day threats that evade traditional defenses, whether they come in through the perimeter, from mobile devices.	
30.	The comprehensive network visibility and security intelligence should be provided by the Solution that covers all areas of the network from internal users surfing the Internet to virtual systems in the data center to eliminate blind spots and improve risk posture. With this advanced insight, organization can detect a wide range of data center issues, from malicious insiders attempting to infiltrate sensitive data, to malware spreading internally from host to host.	
31.	Solution shall combine packet-based/ flow-based monitoring with network behavior anomaly detection to provide enterprise-wide visibility into host and network behaviors, adding a broader context around point-in-time security events.	
32	Solution must monitor users and mobile devices on the network, including personal smartphones, tablets, and laptops. Mobile awareness helps pinpoint the exact source of issues such as zero-day attacks, insider threats, policy violations and data leakage.	
33.	Solution should provide a complete picture of everything happening on the network to deliver the situational awareness needed to maintain high levels of security and performance amidst a constantly evolving network and mobile environment.	
34.	By collecting, analyzing, and storing large amounts of packet/ flow data, the solution should provide a full audit trail of all network transactions for detecting anomalous traffic and performing more effective forensic investigations.	
35.	Solution must deliver unparalleled levels of visibility, accountability and measurability into both individual host and broad network communications required for achieving and maintaining compliance with industry and government regulations. Advanced levels of context including identity, device and application awareness, as well as user-centric monitoring features, further enhance audit controls for regulatory compliance.	
36.	Through continuous network monitoring, the solution should ensures network and application availability and internal security through enhanced network visibility	
37.	Provides user accountability for security and network risks through network visibility and authentication stores.	
38.	Supplies risk measurement, prioritization and optional mitigation through network visibility and customizable thresholds	

	Solution should provide application bandwidth utilization graph for various applications which should include bandwidth consumption trends on network bandwidth utilization.	
	Solution should probe the network in a manner so that impact on network performance is minimal.	
39.	Should support out-of-the-band/ offline modes.	
40.	The tool should have a system for interactive event identification and rule creation.	
41.	Devices those do not support flows, the solution should be capable to generate its own flows for monitoring.	
42.	Solution should have facility to assign risk and credibility rating to events.	
43.	The solution should support traffic being mirrored from switches to a single or multiple sensor appliances with supports of up to 30 Gbps of throughput, and the sensor appliance(s) will generate flow information from the captured traffic.	
44.	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 or in case of packet data it should show the entiere bid-directional communication flow.	
45.	The solution should be able to stitch flows into conversations even when the traffic is NATted by the firewall; clearly showing the original and translated IP address in case of packet based solution it should show the entire bid-directional communication flow.	
46.	The solution should be able to visualize malware propagation behavior.	
47.	The solution must distinguish between similar devices based on unique fingerprints (including unmanaged & IOT) and provide commonality & frequency analysis for each such fingerprint to minimize the false positive rate. Must automatically group similar devices together based on a combination of fingerprints, provide an explanation of the similarity, and identify packet captures/ Flow corresponding to that fingerprint for forensic and outlier analysis.	
48.	The solution should support and provide examples at a minimum, all of the following data science methods. Details with examples on how each of these data science methods are used should be provided and demonstrated as part of the proof of concept evaluation if required like: ● Supervised machine learning ● Unsupervised machine learning	

49.	The solution shall provide minimum 75 Days retention of the flow records/packets to aid in the discovery of low-and-slow attacks.	
50.	The solution should provide capabilities to provide threat detection techniques (models/Rules/ML/etc) and allow for their easy modification or adaptation or alert creation based on the traffic detected.	
51.	OEM should have India based TAC support center. Proposed solution should support 24x7x365 OEM TAC support and Next Business Day Hardware replacement.	
52.	The Solution proposed by the bidder for NBAD/NDR must have 3 references in India.	

Item No. 5: DNS Security

Make & Model offered:…… (need to be filled by the bidder)

Sr. No.	Minimum Feature Requirements	OEM Compliance (Y/N)
	Architectural Requirements	
1.	The proposed solution must be able to provide cache, recursion & Internal Authoritative DNS solution in HA.	
2.	The solution must have DNS security license for 10,000 users or 100000 QPS from day one, user can be remote and/or on-premises.	
3.	The solution must have a minimal impact with the existing DNS infrastructure, requiring no physical hardware installation and using the existing Internet infrastructure OR The proposed solution should be an appliance-based solution; it shouldn't have any limitation for handling internet traffic up to 30Gbps.	
4.	The solution must offer several deployment options: such as an internal virtual forwarder, pointing the forwarder of the existing authoritative DNS to the recursive service, pointing the DNS configured on the Internal Proxy to the recursive service, or also an agent on the endpoint, without any additional physical hardware.	
5.	The DNS security service must be provided via a global data center network OR on proposed appliance.	
6.	The solution must be applicable simultaneously to corporate users connecting from wired and wireless networks, with the possibility to define different policies based on different public Ip's or internal networks	
	Security Requirements	
7.	The solution must be able to detect and block advanced malware related domains regardless of the specific ports or protocols used by the malware OR must be able to integrate with any third-party reputed DNS Block list (to be included as part of offering)	
8.	The solution must be able to block malicious domains using protocols different from HTTP / TLS (DoT)/ DNS over HTTPS (DoH).The solution must be able to block at least from the following categories of malicious domains: botnets, exploit kits, drive-by, phishing, newly seen domains.	
9.	The solution must be able to prevent infections, blocking the DNS requests towards malware distribution domains or drive-by	

	domains, and contain the pre-existing infections, blocking the DNS requests towards command-and-control infrastructures. The solution should support following Feeds :- • Malware Domain and IP • DGA • Ransomware Domain and IP • Bogon Domain and IP • DOH Domains and IP • Bot IPs • Exploit Kit IPs • Malware DGA hostnames • TOR Exit Node IPs • Eastern European and Chinese IP (EECN) • Cryptocurrency hostnames and domains • Newly Observed and Zero day Domains	
10.	The solution must be able to support DNS Filtering for User using Domain Categorization. OEM must have tool that security analysts can use to report on why domains were classified as malicious by the DNSFW/threat feed (Threat Lookup)	
11.	The Solution must support Application discovery in DNS Security. The solution must have ability to detect which type of application is accessed by organization user and must have ability to allow or block the usage based on review or organization policy.	
12.	The solution must leverage predictive intelligence and not just use static signatures or blacklists.	
13.	The solution shall provide shared threat intelligence which can be consumed by other security solution like Next-Gen firewall, SIEM, Proxy etc. The threat intelligence shall be consumed using various interfaces like API, TAXII, JSON etc.	
14.	The threat intelligence must be automatically updated in less than 15 minutes after the discovery of a new threat without any manual update operations.	
15.	The vendor shall have an in-house threat research team to provide real-time intelligence and not depend on third party feeds or lists.	
16.	The proposed solution shall also protect users when they are outside of enterprise network and regardless of where they connect from, so far as they're using corporate asset to connect to internet.	
	Management Requirements	
17.	The management interface must be web-based with a multi-tenant architecture. It must allow to create different user profiles with different level of permissions. As an example, the roles must	

	include: ▪ Administrator ▪ Reporting User Read-Only Users	
18.	The policy editor must allow the creation of security policies.	
19.	The policy editor should allow to define a blocking page for the blocked DNS connections.	
20.	It should be possible to customize the blocking page for each policy entry. The customization must include the ability to define a custom message, insert a custom logo, or an administrator email address.	
21.	The policy editor must allow to forward the blocked connection to an internal URL or domain.	
22.	The events related to all the DNS queries analyzed must appear in real time, with the ability to configure filters based on destination, source IP, response type and date.	
23.	The Solution must support the prevention from Data Exfiltration over DNS with Behavioral Analysis / DNS Tunneling VPN	
24.	The Solution must support the Security policy to prevent from Domain Generation Algorithm based Attacks.	
25.	The Solution should have security policy to prevent from DNS Based Fast Flux attacks.	
26.	Proposed solution should provide SOC team capability to access threat intelligence for view of relationship between domains, IP and malware for investigation. • Proposed solution should provide dashboard which allow the manual submission of domains, IPs, email addresses, ASNs and hashes for investigation by IR team.	
27.	The management platform must have advanced reporting capabilities in order to determine which services are used inside the organization by traditional or embedded devices and eventually detect anomalies in their usage.	
28.	All the activities made by administrators must be logged inside an Admin Audit Log Report	
29.	The solution must be able to apply an additional level of enforcement based on the analysis of the connections trying to connect directly to an IP without generating and DNS queries.	

30.	The management platform must allow to generate the following reports: ▪ Total requests ▪ Activity volume ▪ Top Domains ▪ Top Categories ▪ Top Identities	

Item No. 6: Anti-Advanced Persistent Threats solution (APT)

Make & Model offered:…… (need to be filled by the bidder)

S.No.	Specifications Required	OEM Compliance (Y/N)
1.	The Web - APT solution offered should be an on-premise appliance based solution deployed in inline mode and the traffic should be allowed to pass through, in case, of any hardware failure of the APT solution.	
2.	The Anti APT appliance should inspect the web sessions HTTP traffic to detect and notify the malicious web activity including malicious file downloads through the web/internet.	
3.	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active in DC Environment.	
4.	The Anti APT appliance should stop web-based attacks and have capability to prevent outbound multi-protocol call-backs of the malware with end to end throughput upto 12 Gbps for DC and 5 GBPS for DR site. Solution should be deployed in inline mode as a dedicated appliance sensor monitoring user segment traffic as well as dedicated appliance sensor for monitoring data center segment with each device individual device/ sensor supporting upto 12 Gbps for DC (RSDC-Jaipur) and 5 GBPS for DR site (RSDC- Jodhpur) Throughput and 80,000 concurrent users / a minimum of 4 million concurrent connections and 150,000 connections per second.	
5.	The proposed solution should have the ability to analyse, detect and block malware in common file formats namely executables, JAVA, PDF, MS Office documents, common multimedia contents such as JPEG, QuickTime, MP3 and ZIP/RAR/7ZIP/TNEF archives, 3gp, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm etc. to prevent advanced Malware and Zero-day attacks.	
6.	The solution shall perform analysis on premise and no information shall be sent outside the RSDC network where the same is deployed for data privacy	
7.	The solution should store payload and artefacts of the detected threats for further analysis and incident timeline analysis	

8.	The solution shall report source IP, destination IP, source port, destination port and complete URL of the attack. The solution should also assign a unique identification number to each identified/detected threat for future reference.	
9.	The solution shall detect the entire infection lifecycle and provide stage-by-stage analysis of the attack starting from system exploitation to data exfiltration	
10.	The solution shall provide Risk-based alerts/ logs	
11.	The solution should have ability to block all outbound call-back communication initiated by the internal infected clients	
12.	The APT solution should support integration with popular network forensics tool and SIEM.	
13.	The solution should support the ability to alter priority of dynamic-analysis environment execution for certain IP addresses	
14.	The solution should support SNMP, syslog for integration with a SIEM Solution	
15.	The solution should support at least 80,000 concurrent users or a minimum of 4 million concurrent connections and 150,000 connections per second from day one.	
16.	The solution should have no dependency on any other network device (e.g. Firewall, IDS/IPS, any type of security gateway, etc.) for its functioning. The capability should not be bundled as a part of proposed UTM/ Firewall, Anti-Spam, IPS, or integrated security solution. Solution should be capable of working independently even if other layers of infrastructure change in future.	
17.	The proposed solution should have the ability to be deployed in the following modes: Inline blocking inline monitoring and, SPAN mode	
18.	All necessary additional devices, licenses required for such configuration should be quoted as part of the solution	
19.	Ability to fully forensically analyse identified malware and provide the following information to enterprise staff: Comprehensive Host Modification Report Copy of malware binary(s) PCAP of all Malware Communications to Malware Command & Control servers Full URL trails identifying all of the locations to which the malware attempts to communicate.	
20.	The solution must utilize purpose built Virtual Machine (on-premise) to positively identify malware, including zero hour vulnerability exploits, polymorphic payloads, and obfuscated java-script.	

21.	The APT solution should have concurrent execution of at least 475 virtual machines to enable parallel analysis of multiple objects coming in the web traffic stream without impacting performance for DC and at least 200 virtual machines to enable parallel analysis of multiple objects coming in the web traffic stream without impacting performance for DR. This may be achieved using a single or multiple appliances stacked/ clustered together.	
22.	The solution must be able to detect and report malware by using multiple operating systems VM's (with multiple service pack levels) supporting both 32-bit and 64-bit operating system.	
23.	The solution shall support XFF (X-Forwarded-For) to identify the IP address (internal LAN IP address) of a host in a proxy environment	
24.	The solution should provide a Dashboard that offers real time threat visibility and attack characteristics	
25.	The solution should be able to schedule reports and provide the flexibility to generate on-demand reports.	
26.	The solution should provide reports in (not limited to) HTML/CSV/PDF/XML Formats	
27.	The solution should support logging of important parameters like Source IP, Destination IP, ports, protocol, Domain, time stamp etc. of the malicious web sessions	
28.	The solution should support LDAP or RADIUS & Local Password authentication schemes	
29.	The solution should have the ability to provide for online / offline updating of threat intelligence.	
30.	The solution should support Remote administration using both SSH and HTTPS.	
31.	The Anti APT appliance must be able to detect and report web exploits by using multiple versions of web browsers and plug-ins.	
32.	The inline blocking function of the Anti-APT appliance should be self-contained, and should not contingent upon integration with third-party firewalls, intrusion prevention systems, or other security tools.	
33.	All components of solution should be a dedicated hardware appliance	
34.	The Web APT solution should have anti-evasion technique based hypervisor/ visualization solution.	
35.	The Web APT solution should be able to notify an end-user by displaying a comfort page when traffic is blocked owing to the presence of an infection.	
36.	The proposed solution must be able to run multiple Micro Tasks in a single VM (e.g. run sample across multiple versions of Adobe Acrobat in a Single VM Execution)	

37.	The solution must include prepopulated LICENSED copies of Microsoft windows and office images through an agreement with Microsoft. There should be no requirement for the customer to buy additional Microsoft licences for sandboxing solution	
38.	APT appliance solution must be deployed in inline block mode and solution should be designed for the same	
39.	Appliances should be capable of handling 80,000 Concurrent Users or should support a minimum of 4 million concurrent connections and 150,000 connections per second from day one.	
40.	Data Ports: 4 x 10G interfaces. Management ports: Minimum two number of 1G Copper ports.	
41.	SSD: 4x 4TB, RAID 10 or higher, with support for hot-swappable drives.	
42.	Rack Mount: Rack mountable with OEM Rack mounting kit	
43.	Throughput: The solution should be able to handle 12 Gbps for DC and 5 GBPS for DR site.	
44.	Power Supply : Dual Power Supply	
45.	All necessary appliances, licenses required to meet RFP requirements should be quoted as part of the solution	
46.	Proposed APT Solution should have centralized management console deployed to manage configuration of all connected APT devices centrally	
47.	Central Management Console should have ability to centrally deploy the updates, patches and security contents/updates to all connected appliances	
48.	Central Management Console should have ability to upgrade VM Guest Images centrally on connected APT sandboxing environment	
49.	Central Management should help in identifying which APT device is running at lower version and needs to be updated	
50.	Centralized Management System should have web based GUI and a unified security dashboard displaying the real time consolidated data in graphical/textual format and all alerts received from and detected by APT devices. Central Management should help in providing centralized alert view for all connected APT devices as well as capability to group devices view all alerts or specific to an appliance	
51.	Central Management system shall provide consolidated alert reports in various formats	
52.	Central Management should be able to distribute local generated threat intelligence among other APT devices connected such that if One APT device detects unknown threat locally that intelligence can be shared with multiple other APT device connected through central console for faster detection	

53.	Web APT solution must be able to detect zero day attacks and generate local blocking rules or signatures on APT device itself that should block subsequent call-backs or infection URL that match locally generated signature. The solution must be able to auto-generate local rules (local infection, local call-backs) after completing dynamic analysis on premise on the appliances itself so that it can start blocking zero day malicious URLs and call-backs.	
54.	Virtual Execution or Sandboxing component should be secure hardened hypervisor and should not be from list of COTS hypervisor like VMWare, Hyper-V, Citrix, Oracle etc. since advance malware can easily make out when executed in COTS based hypervisors do not show behavior leading to poor detection & False Negatives. This is critical hence detection engine should be resistant to VM evasion techniques used by advance malware in APT attacks.	
55.	The solution must be able to detect multi-flow web-based attack where multiple files are executed in flow in attack. Please provide any case study where vendor publically detected multi-flow APT zero day attack.	
56.	3 years OEM comprehensive Onsite Warranty and support for both hardware and software (24x7)	

Item No. 7:

(A) SIEM with UEBA & Integrated with Network forensic (Packet Capture and Re-Construction Capability)

Make & Model offered:…… (need to be filled by the bidder)

Sl. No	Minimum Feature Requirements	OEM Compliance (Y/N)
1	The proposed SIEM solution should be in Gartner's Leaders Quadrant at-least twice in last 5 years.	
2	The proposed solution must include Next Gen SIEM, Security Analytics, Big Data Analytics with necessary automation capabilities. To avoid maintaining multiple data repositories, proposed solution should have central data repository which should act as common data lake for SIEM, UEBA & SBDL	
3	The proposed solution must have Big Data Platform and should support horizontal and vertical scaling for further growth.	
4	The proposed solution must support 1200+ integration available out of the box by the solution. OEM to provide parsers for data ingestion for all the current data sources and their respective upgrades (in maximum 15 business days from data of intimation of the same) during the contract period. If any new data source is added during the contract period, the OEM will provide parsers for data ingestion in maximum 15 business days from data of intimation of the same, without dependency of the bidder.	
5	The proposed solution must support the collection of the Net flow/Sflow logs without additional appliances or components	
6	The proposed should provide integration with any File Integrity Monitoring (FIM) through supported integrations of the same NG-SIEM platform.	
7	The proposed solution must have 1000+ out-of-the-box use cases such as MITRE, Ransomware, UEBA, NTBA, PCI, Insider Threat, NDR etc..	
8	The platform must provide predictive Threat Intelligence Using Behavior Modeling	
9	The solution should be implemented on Hardened OS and database in Hardware. The hardware configuration must be able	

	to handle and store the peak load of 2,60,000 EPS/7.5 TB of load at anytime from the day one itself for the retention period defined	
10	The Solution should provide web-based administration (https)/ user interface for device management and monitoring.	
11	The system should be able to capture information about criticality ratings of assets and should leverage that information while performing correlation and raising alerts/incidents.	
12	The vendor should facilitate that in case of failure of assigned collector, the devices should be able to send the data to another collector (if available) without losing any data so that there be no gaps in analysis and reporting. In case the connectivity with SIEM management system is lost, the collector should be able to store the data in its own repository. The retention and synchronization with SIEM database should be possible automatic but configurable for this repository	
13	The solution should support correlation of logs from all the devices within an enterprise and all security scenarios like spoofing, authentication failures, etc. The solution must support multi-device, multi-event and multi-site correlation across the enterprise. The solution should be able to correlate on any fields in raw data.	
14	The proposed solution should be able to trigger actions. These actions can be automatically triggered by correlation alerts or offences or manually run on an ad hoc basis from the Incident.	
15	The proposed solutions should use multiple technologies like using distance formula, geo Database, etc. to detect geographically improbable access	
16	Solution should integrate with major threat intelligence from both open source and commercial intelligence feeds for botnet C&C servers, malware domains, proxy networks, known bad IP's and hosts, traffic to APT domains	

17	The proposed solution's detection use cases should be comprised of guidance that provides an assessment of the Security Threat and how it helps detect and investigate it using the proposed solution. In addition, it should provide a summary of how the attack or detection technique maps to the following: ATT & CK MITRE, an adversary behavior model that describes the actions an adversary might take. Kill-Chain, a model that identifies the phases an adversary must complete to achieve their objective. CIS Critical Security Controls Data types that are referenced within the rules/ search and that need to be populated. Technologies, example technologies that map to the data types. There should be template to upload advisories in an automated manner. There should be templates to design and trigger work flows automatically. Any other customizable templates as per the requirements.	
18	The proposed solution must offer all the reports/compliance package reports out of the box at no additional cost.	
19	The proposed solution must come with out-of-the-box integration and dashboards, reports, rules etc. to provides rapid insights and operational visibility into large-scale CentOS, Windows, Unix and Linux environments machine data: syslog, metrics and configuration files.	
20	SIEM solution and corresponding hardware must be able to handle load for the peak performance for the below mentioned EPS log volume: 1. The solution proposed should collect and analyze audit trails logs and NetFlow information (all types of logs – ODBC, SDEE, Syslog, Checkpoint etc.) to detect malicious or abnormal events and raise the alerts for any suspicious events that may lead to security breach in the scoped environment. 2. The solution should be provided in as a software based deployable on the required hardware to handle the peak load at any given point of time . 3. The proposed solution should collect and correlate logs for 2,60,000 EPS /7.5 TB per day without dropping or queuing of logs across all layers and there should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be	

	integrated. 4. The solution should provide an integrated dashboard and analysis system that could provide a single view into all the analysis performed across all the different data sources. 5. The following devices/security solutions are presently deployed from which data need to be collected for analysis using either agent based or agentless mechanism a. Network Firewall (Perimeter + Zonal) + WAF b. IPS + DDoS c. MS-Windows Servers d. Linux Servers (RHEL, Ubuntu) e. Switches f. Routers g. Web Content filtering solution/ UTMs h. Anti-Virus i. APT solution j. Forensics solution k. Any other SNMP enabled device.	
21	1.The proposed solution will be continuously used in the SOC so that solution builds specific repository which includes categories like including event types, tags, lookups, parsing/normalizing, actions and saved searches etc. It should help to discover and analyze various aspects in data. For example, event types should enable analyst to quickly classify and group similar events; then use to perform analytics on events. 2. The solution should perform comprehensive Risk Ranking for not just users but also for entities, network & IPs, applications , country ,users and related activities and should uniquely stitch multiple individual risk based alarms to identify which user/entity has more alarms against it and that would naturally translate into a higher risk ranking. 3. The proposed solution must support the retention of logs and data. The retention period for raw logs and their associated normalized events is 180 days (Searchable logs), with 365 days for archival storage. For searchable logs, the first 90 days must be stored on SSD/NVMe, and the subsequent 90 days on SSD/HDD. 4. The proposed solution should have the capability for the retrieval of data from archival storage within 48 hours from the date of request. Hardware and configurations to be considered by the SI.	

22	The proposed solution must be able to handle peak load for logs of 2,60,000 EPS /7.5 TB per day anytime from the day one without dropping or queuing of logs across all layers and there should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.	
23	3 years OEM comprehensive Warranty and support for both hardware and software (24x7)	
UEBA		
24	Solution should be based on unsupervised machine learning/deep learning so that it does not require any human/analyst to create data science models.	
25	Solution should have all the behavioral detection models OOTB without any need of a data scientist	
26	The proposed solution should natively have ML/deep learning capabilities and should not have separate engine/compute requirements for running ML models.	
27	The UEBA must be able to monitor all the users and entities in the organization covered by the SIEM solution which is equal to 1,00,000 Users + Entities / 2TB per day. UEBA should not have separate data repository and should consume and operate on data lake or SIEM data repository.	
28	The UEBA must create a heuristic baseline of user activity by analyzing behavior, so it must perform multidimensional baselining, enabling the modeling of a broad set of user behaviors. Baselines are used to detect anomalous behavior via machine learning/deep learning and other statistical analysis techniques.	
29	Solution should support user and entity-based behavior Analytics	
30	Solution should not depend only on event log data. it must leverage network full packet capture and endpoint system level activities to gain comprehensive visibility,	
31	To be able to correlate across user access logs, network access traffic and endpoint activities and apply data science models to detect those abnormal user and entity behaviors occur anywhere in the network	
32	Solution should be an integral component as part of SIEM and should have same UI as the SIEM solution to provide event level and historical level analysis along with behavioral analysis	

33	Indicators falling under following high-level threat categories must be detected across endpoints, network traffic and user activities: · User Logins to Multiple AD Sites · User Login to Abnormal Host · User Logged into Multiple Hosts · Snooping User · Sensitive User Status Changes · Registry Run Keys & Start Folder · PowerShell & Scripting · Non-Standard Hours · Multiple Logons by User · Multiple Failed Logons · Mass Permission Changes · Mass File Rename · Mass Changes to Groups · Elevated Privileges Granted · Discovery & Reconnaissance · Data Exfiltration · Credential Dumping · Admin Password Change · Abnormal File Access · Abnormal AD Changes · Phishing · Data Exfiltration	
34	Machine learning/Deep Learning should be embedded across the platform (SIEM, SBDL & UEBA). It should empower every user in the SOC with ML. Security analyst to become citizen data scientist i.e. used predefined ML algorithms to detect & predict threats, threat hunters to build their own ML models with steps to build, train and implement model and data scientists should be able to integrate various ML frameworks.	
35	Provide an aggregated analytics UI dashboard to security analysts with ability for detailed drilldown investigation of specific events.	
36	Solution should be able to track user's activities locally and remote network sites and should be able to report usage behavior across the entire network.	
37	Solution should have facility to assign risk and credibility rating to events.	
38	Solution should support Machine Learning (ML)/Deep Learning driven risk scores and risk profiles for user.	

39	UEBA should be a pure unsupervised machine learning engine with no need to configure any settings not limited to baselines, thresholds, decays, risks scores. Also, there should not be any need to configure thresholds through settings during learning or production phase	
40	Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields	
41	Behavioral analysis solution should have embedded machine learning engine and there should be no separate app/plugin for same	
42	The User and Entity Behavior Analytics solution must be integrated with SIEM, and leverages available Logs, endpoint (EDR) data for its behavior analytics.	
43	The proposed solution must be able to handle peak load for logs of 2,60,000 EPS /7.5 TB per day anytime from the day one without dropping or queuing of logs across all layers and there should not be limitation on the number of devices like servers, network devices, virtual machines or any other data source(s) that is required to be integrated.	
44	Proposed solution should leverage the data in SIEM platform and not build its own data store and maps the fields in the data to UEBA-specific fields.	
45	The UEBA must be able to monitor all the users in the organization. UEBA should not have separate data repository and should consume and operate on data lake or SIEM data repository. Use Case: Every single user can be source or a target of threat hence it's very important to cover all the users with UEBA solution.	

(B) Network forensic: Packet Capture and Re-Construction Capability

Make & Model offered:…… …… (need to be filled by the bidder)

Sl. No	Minimum Feature Requirements	OEM Compliance (Y/N)
1.	Should be an OEMs on-premises purpose build appliance-based solution with capability to do complete packet capture, storage, dissection for 700+ protocols/parsers, generate meta ,root cause analysis, artefact timelines in a single solution.	
2.	Should support multiple ingress interfaces for capturing from multiple network points and should be capable to capture lossless packets and store for 15 days minimum and to support as per below: **(RSDC- Jaipur)** · DC: 7GbPS sustained performance with up to 12 GbPS peak · Seclan: 4GbPS sustained performance with up to 6 GbPS peak **(DR- Jodhpur)** · DR : 4GbPS sustained performance with up to 6 GbPS peak	
3.	Should capture all packets from network in real time and be able to classify, extract and analytics, reconstructs the data, analysis of network activity and forensics over IPv4 and, IPv6	
4.	Should be able to provide complete packet-by-packet details pertaining to one or more session of interest including voice/video replay / decode, page reconstruction, image views, artifact & raw packet extractions and indexing of URIs from emails / Packet Decode.	
5.	Should have Hardened Database and be able to handle IOPS required for the solution so not to allow any latency. To ensure disk IO performance, the raw traffic and the metadata should be stored on separate disks/appliances, and they should be managed with separate storage capacities and periods.	
6.	Should include Directly Attached Storage as per below: • For DC: minimum 1.2PB capacity after RAID 5 or higher RAID configuration and should be scalable to 2 PB. • For Seclan: minimum 600TB capacity after RAID 5 or higher RAID configuration and should be scalable to 1 PB. • For DR: minimum 600TB capacity after RAID 5 or higher RAID configuration and should be scalable to 1 PB.	
7.	Should have minimum 2 x 1 GbE management and and 4 x 10 GbE monitoring/capturing interfaces. Data stored by the solution should be encrypted. SSD/SAS to be used for the execution of the dashboard and its indexing. For packet data solution should use the SAS drives	

8.	Proposed solution should extract the attributes of a network session in the form of a meta [Like IP source, Destination, Country, Mac Address etc.…] from both header and payload of all common network protocols	
9.	Offered product have Common Criteria (EAL-3+/PP) / FIPS 140-2 certification.	
10.	Should be able to filter the captured packets based on layer-2 to layer-7 header information.	
11.	Should provide comprehensive deep packet inspection (DPI) to classify 700+ protocols/Parsers and can be customized for parsing of unknown protocols.	
12.	Should have capability to upload packet captures (PCAP's) captured elsewhere for packet analysis.	
13.	Should have capability to download specific session packets without size restriction.	
14.	Should do multi-dimension indexing of packets based on layer-2 to layer-7 header information.	
15.	Should provide classification, search and real-time file extraction for instant delivery of recognizable evidence of a security breach or malware attack.	
16.	Should have REST-API for integration with other Security Solutions and Direct integration with leading SIEM and dynamic analysis tools.	
17.	Solution should provide root (super-user) access out-of-the-box to the buyer and be able to provide access to packet captures and forensics information from within the root shell.	
18.	Should have inbuilt packet analyzer accessible in single console to see the data.	
19.	Should support extracts and analyses any file—including the most prevalent and malicious file types using inbuilt feature or integration with sandbox.	
20.	Should have ability to integrate with reputed threat intelligence Feeds for artefact analysis.	
21.	Should have inbuilt tools or can be integrate with external tool for static analysis (such as jsunpack, yara, etc.) of files/artifacts.	
22.	Solution should integrate with on premise open-source or commercial dynamic- analysis tools to detect unknown threats.	
23.	3 years OEM comprehensive Onsite Warranty and support for both hardware and software (24x7)	
24.	The solution should support selectively discarding, masking, or filtering packets based on their security relevance (e.g., customer PII, SPDI, etc.)	
25.	The proposed solution should ensure lossless packet and payload capture with network inflow/outflow of data.	

26.	"The proposed packet capture solution should be able to perform real-time monitoring and network traffic analysis to identify threats. The solution should feature Deep Packet Inspection (DPI) to provide visibility into all layers of the OSI stack (L2 to L7), including application payload data, but only for suspicious and malicious traffic. The solution should create indexes for payload objects as required and not just rely on header information." Additionally, the solution should provide network traffic insights by: a. Classifying protocols and applications b. Performing deep-packet inspection c. Supporting cross-correlation for analysis and aggregation d. Reconstructing sessions and analyzing artifacts e. Previewing artifacts and malicious attachments	
27.	"The solution should possess the capability to extract data / malicious files from the captured network packets. Additionally, the solution should include the functionality for comprehensive session investigations, as well as packet analysis on the captured packets and any generated alerts."	
28.	The solution should have the functionality to reconstruct for complete packet analysis or replay/decode the network packets which will help to identify the entire transaction.	
29.	The solution must be capable of capturing and recording all network packets in full (both header and payload). Additionally, the solution should provide the flexibility to selectively save packet data based on specific applications, protocols, time durations, or a combination of these criteria. For each application traffic flow, the solution should support the following capture options: - Full Packet Capture: Capture the entire packet, including both header and payload information. - Packet Truncation: Capture only a specified portion of the packet, reducing storage requirements while preserving essential data. - Packet Exclusion: Exclude specific packets based on defined criteria, such as application, protocol, or source/destination addresses. - Header-Only Capture: Capture only the packet headers, providing basic information without the full payload.	
30.	The PCAP solution should be capable of capturing network traffic and flexibility to use tools to read / extract pcap files on the device itself rather than downloading it to local machine.	
31.	Proposed solution should have below features: - Zero-Day Threat Detection: The solution must be capable of identifying and mitigating zero-day threats as they emerge, ensuring proactive	

	protection against emerging cyberattacks. - Retrospective Analysis: The system should allow for in-depth examination of captured packets, enabling the extraction of valuable metadata for subsequent analysis by an analytics engine. - Packet Storage and Analysis: The solution must have robust capabilities for storing, extracting, and analyzing packets, providing essential insights for incident response and threat intelligence.	
32.	Proposed solution should have below search capabilities: - Efficient Indexing and Searching: The solution must have robust indexing and searching capabilities to allow for quick and easy location of specific packets based on a wide range of criteria. - Search Criteria: The solution should support searching based on various criteria, such as time, links, IP addresses, port applications, protocols, and any other relevant attributes.	
33.	The solution should be able to detect and analyze the following incident categories (but not limited to): - Suspicious communication over non-standard ports - Data exfiltration attempts - Command and Control (C2) communications - The use of The Onion Router (TOR) - SSH communication with monitored countries - Privacy VPN usage detection - Reconnaissance activities - Detection of unknown Domain Generation Algorithm (DGA) attacks	
34.	The solution should be able to generate alerts for all above mentioned detection with proper investigative work flow with Host Analysis, Session and packet analysis	
35.	The Solution should detect common events like D-DOS / DOS, Scanning, Worms, Unexpected application services. (e.g., tunnelled protocols, backdoors, use of forbidden application Protocols), Policy violations, etc using IOCs & various detection methods. The solution should profile traffic by TCP and UDP Port.	
36.	It should be able to search metadata items such as IP address, hostname, user account, command, email, filename, server name, client name, etc. based on the index. The system should provide a feature to extract various types of files from network traffic (.exe, .pdf, .doc, .gif, .jpeg, etc.).	
37.	Capable of protection against advanced attacks and malware types that are difficult to detect via signatures like web shell uploads, existing web shells, ransomware, cryptominers etc.	
38.	Provide visibility to various types of network anomalies and suspicious activity such as Data Exfiltration, Beaconing, etc. and their victim attacker	

	graphical representation at one place, Detect malicious TLS connections, must provide full Detection, Network Visibility, Investigation & Forensic capability, through high speed lossless packet capture & analysis functions for a network traffic capture	
39.	The Investigation features should be provided the capability to perform complete network forensic investigations or The Investigation features should be provided the capability to perform complete network forensic investigations including decoding and chaining the encoded communication traffic. Also, the solution should be providing download option of select and/or bulk pcaps in industry standard formats like "pcap".	
40.	Detect zero-day, multi-stage, fileless and other evasive advanced attacks using dynamic, signature-less analysis. The Internal Network Analysis solution should also be able to detect malicious post- exploitation activities such as attacker lateral movements between various zone like user workstation & servers. The solution should detect lateral movement indicating source & destination IP addresses.	
41.	The Investigation features should be provided the capability to perform complete network forensic investigations or The Investigation features should be provided the capability to perform complete network forensic investigations including decoding and chaining the encoded communication traffic. Also, the solution should be providing download option of select and/or bulk pcaps in industry standard formats like "pcap".	
42.	Solution should analyze following application types: a. Web pages: HTML, HTTP--GET, HTTP--POST, HTTP--RESP b. Email and attachments: EML, SMTP, POP3 c. Document files: DOC, DOCX, XLS, XLSX, PPT, PPTX, PDF, WPD d. Images: JPG, BMP, GIF, PNG e. Config, system files: REG, DLL, CONF, CPP, ELF, EXE f. Compressed archives: ZIP, GZIP, RAR g. Core Services: SNMPv1-3, AD, DNS, DHCP, NTP, LDAP, FTP, TFTP, SMB v1/v2, SCP h. Voice & Multimedia Application : SIP, H232, RTP, SCCP, MSRP and Video: H.323 etc. i. Remote Desktop: Microsoft Remote Desktop, Citrix ICA, VMWare and Citrix Channel j. Routing and others: Syslog, OSPF, BGP,AD, DNS, DHCP, NTP, LDAP, FTP, TFTP, SMB v1/v2, SCP	

43.	Proposed Network Threat Detection platform should adopt technics to provide visibility into channels that are trying to blend in with other traffic, but do not follow normal protocol behaviour. Proposed solution should understand the behaviour of the protocol and highlight in case of any discrepancy. The solution must be capable of identifying suspicious or hitherto undiscovered communication patterns.	
44.	Solution must have reconstruction feature from day one for DPI and solution should be capable of doing full session reconstruction at the point of capture from raw packets to meaningful artefacts like email, FTP data files, PHP, JavaScript and .Net files. Also, post reconstruction solution should be able to do object extractions from sessions like pcaps, zip files, office documents, embedded malicious attachments etc.	
45.	Network traffic inspection to detect suspicious activities such as different malware family used by Threat Actor groups, TTPs used for malicious activities and lateral movements or The solution should detect and respond to threats based on MITRE ATT&CK tactics and techniques and report the appropriate MITRE ATT&CK tactic and /or technique in the platform user interface.	
46.	The system should provide a feature to instantly decode and display Base64 and URL-encoded data.	
47.	To protect personal information, the system should provide a feature to provide hashing certain metadata such as email addresses, user accounts, etc. for certain users.	
48.	To guarantee search performance, the disk used for storing search indexes should be provided with an SSD.	
49.	All disks of the appliance and the storage should be from same OEM and should utilize Self- Encrypting Drives (SED) or using any encryption tool/methodology to keep data safe.	
50.	When extracting files from reconstructed session, Solution should have a function to authorized user to perform the extraction with strong password.	
51.	Solution should allow user to create network parser by doing minimum effort on the platform, without the need of learning any programming language.	
52.	Solution should provide out of box integration with MITRE ATT&CK framework to get the details on the attacker's tactics and techniques associated with the alerts/Incidents within the tool, by not going on any external/third party community website.	

53.	Solution should allow to doing response level actions by integrating with security controls such as firewall, SIEM, SOAR etc.	

Item No. 8:

(A)WAF with API Security (For RSDC Jaipur & DR Site Jodhpur)

Make Model offered:…… (need to be filled by the bidder)

Sl. No.	Minimum Feature Requirements	OEM Compliance (Y/N)
1	The Proposed Solution shall be cited within the Leaders segment in the most recent Gartner Magic Quadrant for WAAP.	
2	The WAF Appliance must be a dedicated hardware.	
3	The proposed solution must support the following: 1. DC - 10 Gbps of WAF throughput. In case any OEM/Bidder has L4/L7 throughput mentioned in the Datasheet then the L7 throughput of the appliance must be at least 200 Gbps. 2. DR - 5 Gbps of WAF throughput. In case any OEM/Bidder has L4/L7 throughput mentioned in the Datasheet then the L7 throughput of the appliance must be at least 100 Gbps. The Bidder must provide evidence of asked throughput on publicly available documents at OEM website.	
4	"The solution must have 384 GB RAM or more and should have at least 2 * 4 TB (Raid 1) Hard Disk. for DC and must have 128 GB RAM and should have at least 2 * 1 TB Hard Disk for DR.	
5	The solution must have inbuilt or through external bypass switch bypass segments to ensure that fail open in case of hardware failure.	
6	The appliance MUST NOT USE Hypervisors OR MAY USE its own Hypervisor which should be a specialized purpose build hypervisor and NOT a commercially available hypervisor like XEN, KVM etc.	
7	The solution must support the following deployment modes to protect the application traffic. Both HTTP and HTTPS must be supported in all these modes. Based on the use case RISL may choose to deploy the solution in any of these modes. - Inline Mode - Layer 2 Bridge - Inline Mode - Layer 3 Reverse Proxy - Out of Band Mode	
8	The WAF solution should not be any white labeled or 3rd party WAF solution deployed on any other OEM's hardware/software.	

9	The Proposed WAF Solution should support both a Positive Security Model Approach (A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked) and a Negative Security Model (A negative security model explicitly defines known attack signatures) . The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats	
10	Both Positive and Negative security model should continuously learn the application. Learning should be a continuous process and should not stop after a certain stage.	
11	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	
12	The Proposed Solution should have Correlated Attack Validation capability which examines multiple attributes such as HTTP protocol conformance, profile violations, signatures, special characters, and user reputation, to accurately alert on or block attacks and also to eliminate false positives.	
13	The WAF solution must have an Anaytics Engine that would correlate and distill thousands of security events into a few distinct readable events.	
14	Proposed WAF Solution should have capability to automatic learning should include Directories, URLs, Form Field Values, Whether the field values is numeric/alphanumeric/alphabets, length of the field etc.	
15	The solution must provide the following features and protection. - HTTP (1.x and 2) protocol validation - Web service layer correlated attack validation - HTTP protocol attack signatures - Web service layer customized protection - Cookie signing validation - Anti site scrapping - Web profile protection - Web worm protection - Web application attack signatures - Web application layer customized protection - OCSP protocol validation	

16	The solution must be able to decrypt SSL web traffic that are using Diffie-Hellman key exchange protocols with the WAF deployed in Layer-2 mode	
17	The solution must automatically discover HTTP traffic content type, regardless of the content-type HTTP header. With this capability, WAF should be able to parse and protect HTTP Requests with missing or wrong content-type header	
18	The solution should protect against Deserialization attacks, accomplished by searching for signatures in the 'Request-Content' header	
19	The Proposed Solution should be able to work in High Availability (HA) mode and should be deployable in an Active-Standby & Active-Active in both DC & DR Environments.	
20	The WAF should have high availability in both layer 3 and layer 2 deployment	
21	All the custom policy and signature creation must be done via GUI. There should not be any need to create any advanced policy from CLI.	
22	Proposed solution should maintain the directory of known IDS/IPS Signatures to be used in policies and detect and exploits in near real-time	
23	The solution must have a GUI based option to create policies to detect and block Double encoding attacks.	
24	The WAF solution must be a completely on prem solution with no data going out to the internet except signature updates and OEM software download.	
25	The solution must be able to provide a threat intelligence feed and service based on source reputation. The feed must be provided in near-real time for the following known attack sources: - Malicious IP - Anonymous Proxies - TOR IPs - Geo Location	
26	API Security solution should offer the most Advanced and comprehensive API Security in the Industry. Including API Discovery , Catalogue, Risk Rating , OWASP top 10 API, Vulnerability pre post development for East West traffic	

27	API Security must do Deep Discovery of both External (North South) and Internal (East West) API right up till data type level of each endpoint	
28	API Security solution must detect and classify sensitive data both in the request as well as in the response for both External (North South) and Internal (East West) API Endpoints	
29	API Security must have the ability to identify API that are vulnerable namely Unauthenticated API	
30	API Security must have the ability to detect API Top 10 attacks which includes BOLA, Mass Assignment, BFLA,Broken Authentication	
31	API Security should be able to run Vulnerability Test on the API Endpoints with or without integrating with any VA Tool.	
32	API Security should have the ability to integrate with On Prem WAF natively.	
33	The solution should be able to block even the most advanced bots that try to emulate standard client behavior and pretend to be web browsers.	
34	The API Security solution should be fully integrated with the On Prem WAF system from the same vendor or should be within On Prem WAF appliance.	
35	The solution should have the ability to provide a threat intelligence feed and service dedicated for bots protection. This threat intelligence service must provide the following capability and data: - Bot Classification of traffic into humans, Trusted Bot, Bad Bot, General Bot and Unknown new bot	
36	The solution should have the ability to provide a captcha service for transaction end points.	
37	Identification should be implemented with the accuracy of the web browser.	
38	The solution must include signature / machine-learning or behavioral analysis mechanisms. They should detect anomalies in the behavior of application clients and classify bots based on similar behavioral patterns.	
39	The solution should also provide protection for APIs that are consumed by browsers.	
40	The system should provide the ability to apply the following actions against traffic classified as BOT: · blocking	

	· monitoring · displaying a captcha	
41	The Bot Component must be able to classify the Bots in the following category: Click Bot, Comment Spammer Bot, Crawler, Feed Fetcher, Hacking Tool, Masking Proxy, Search Bot, Spam Bot, Vulnerability Scanner, Worm, Site Helper and DDoS	
42	The system should have a number of predefined conditions/rules that are most commonly used. It should also be possible to freely define conditions based on logical operators and analysis of attributes acquired during identification.	
43	Part of the product should be a flexible reporting system that can generate various kind of analytic reports alerts being generated. like: • Bad Bot Distribution • Visitor Distribution • List of Top 10 Bad Bot IP • List of Top 10 Bad Bot User Agents • List of Top 10 Unknown Client 1P • List of Top 10 Unknown Client User Agent	
44	The vendor should include the service of a dedicated analyst who has extensive knowledge and experience in configuring WAF and fighting bots. His task will be to analyze the current traffic and assisting in adjusting the configuration to be as effective as possible in the face of ever-changing bot usage techniques and constant changes in the protected application. The analyst should devote a minimum of 8 hours per month to carry out the aforementioned activities.	

(b) DAM (For RSDC Jaipur):

Make Model offered:…… …… (need to be filled by the bidder)

Sl. No.	Minimum Feature Requirements	OEM Compliance (Y/N)
1.	The license must support monitoring of minimum 25 DB Servers	
2.	The proposed DAM solution must support the following databases. 1. Relational Databases e.g - MariaDB, MSSQL, My SQL, Oracle, Postgre SQL. 2. Big Database types e.g Mongo DB	

3.	The solution must have a central Dashboard which shows Activities of all the databases i.e On Prem Databases, Cloud Databases, Software as a Service Databases.	
4.	The solution should help organisations in meeting regulatory compliance such as SOX, PCI DSS, Data Privacy Law, GDPR, Industry best practices, Organization specific security policies etc.	
5.	Solution should capture and analyze all database activities by Database users and/or privileged user accounts, providing detailed audit trails that shows the "Who, What, When, Where, and How" of each database transaction.	
6.	The solution should monitor DDL, DML, DCL, TCL, commands in real-time and It should also monitor user management, privilege management etc. and monitor for any policy violations.	
7.	The proposed solution should support both agent based mode and agentless mode to capture Database Activities.	
8.	In case of agent based monitoring, the solution should not use the native audit functionality of DB Server. In case of Agentless Collection, the native logs of the DB Server must be forwarded to the DAM Solution.	
9.	In case of agent-based monitoring, the solution should support blocking of SQL Queries based on custom criteria like DB User, Column, Table, Query Type etc.	
10.	The Solution must have the option to cap the CPU utilisation of the agents.	
11.	The proposed solution should integrate with 3rd party technologies SIEM, SOAR, Service Management, Ticketing system etc to provide holistic security posture.	
12.	The proposed solution must not use sampling and must capture every log either through Agent or through Native Logs.	
13.	The solution must have playbook which could be used to automate workflows.	
14.	The solution must have the option to define palybooks where a certain action is performed by DAM based on nature of DAM query, e.g locking a user if the user tries to exfiltrate large amount of data.	
15.	The playbook must provide ability to open a service now ticket or a Jira ticket.	
16.	In case of Agents, Gateways / Collectors must be sized accordingly to support 60K TPS/minimum 25 DB irrespective of the type of query. The ability of gateway to support 60K TPS/minimum 25 DB	

	must not depend on whether the query is privileged query or a generic SQL Query.	
17.	The Proposed Solution should support automatic/manual updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats.	
18.	The solution should also discover if any new/rogue database created within the monitored network/systems and alert the respective stakeholders	
19.	The solution should be capable of auto discovering sensitive/confidential data like credit card Numbers, Email address, or any PII in the database.	
20.	The solution should be able to auto discover privilege users in the database and should support user entitlement reviews on database accounts	
21.	The solution must have the ability to create pipelines and use those pipelines in creating custom granular reports, feed data into SIEM , Data Enrichment etc.	
22.	The solution should support creation of policies/rules for enforcing access control and proper rights management on databases.	
23.	Solution should have capability to track execution of any Database Objects stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed.	
24.	The solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc.	
25.	The solution must be able to be used to measure compliance with industry standards and benchmarks such as DISA STIG and CIS.	
26.	The solution should discover misconfigurations in the database and its platform and suggest remedial measures.	
27.	The solution should be able to virtually patch the know vulnerabilities automatically/manually till a patch is installed for the same.	
28.	The solution should verify that default database accounts do not have a “default” password.	
29.	The Solution must provide behavior analytics algorithm to establish behavioral baseline and find deviations	
30.	The Solution must be able to differentiate between suspicious behavior from risky/abusive behavior .	

31.	The Solution should be able to access user's risk potential (compare user suspicious behavior rate to the rest of the organization and etc)	
32.	The Solution should automatically detect the following: a) Nature of accounts which connect to the database (Service Account, DBA User Account.. etc) b) Purpose of database tables (Business Critical Tables, System Tables, and etc) c) Data access habits (working hours, amount of data retrieved)	
33.	The Solution must be able to detect Abnormal Behavior such as: Database Access at Non-Standard Time Database Service Account Abuse Excessive Database Record Access Excessive Failed Logins Excessive Failed Logins from Application Server Excessive Multiple Database Access Machine Takeover Suspicious sensitive system tables scan Suspicious Application data access Suspicious Database command execution Suspicious Dynamic SQL activity	
34.	The Solution must be able to identify/detect the following: a) Typical end point information b) Typical database access patterns	
35.	The Solution should be able to detect suspicious activity including scans for sensitive and valuable data, which may indicate the reconnaissance phase of a potential breach	
36.	The Solution must be able to integrate with active directory to enhance forensics and provide line of sight into user identity.	
37.	The Solution should be able to perform peer group analysis when integrated with active directory	
38.	The Solution should provide context based on user information on AD which include the following widgets a) Employee Details with information such as email, phone numbers and office location. b) Incidents which show a graphical view of the employee's number of incidents by severity. c) Anomalies which show a graphical view of the employee's number of anomalies on a scale of Low to High.	

	d) Endpoints Activity which presents details on the amount of endpoints that were used to access the resources by the employee. e) Databases Activity which presents details on the amount of databases that were accessed by the employee	

Note:

1. All the items of above mentioned should be supplied with OEM Warranty, Support, Subscription/ Software Assurance. (License and asset ownership is required on the date of installation for all OS & related software products)
2. All the supplied Hardware/ Software should be Interoperable, IPv6 ready and in compliance with the policies/ guidelines issued by DIT, GoI in this regard. Also, the bidder is to quote/ propose only one make/ model against item.
3. The quoted components must be supplied as per mentioned validity & support.
4. The quantities are tentative and may increase or decrease as per requirement of the purchaser.
5. All the specifications mentioned above are minimum specifications and higher specifications shall be used wherever necessary/ required. Deviation on higher side shall only be considered and no extra weightage shall be awarded for such deviations. The bidder is required to submit the technical compliance statement for each item only on the respective OEM's letter-head OR email from OEM.
6. Bidders are required to provide a detailed, point-by-point technical compliance statement for the offered product, referencing the tender specifications. Additionally, the technical brochure demonstrating compliance to be accessible in the public domain. Include copies of the technical brochures for the quoted products, where applicable. Simply stating "Yes," "Complied," or reproducing the specifications verbatim throughout the document will not be accepted and may result in bid rejection. Ensure that product data sheets are attached for each relevant parameter, as necessary.

ANNEXURE-3: Bidder's detail {to be filled by the bidder}

Name of the Bidding Company/ Firm:			
Contact Person (Authorised Bid Signatory):			
Correspondence Address:			
Mobile No.		**Telephone & Fax Nos.:**	
Website & E-Mail:			
Bidding document Fee (Tender Fee) details	• Amount: • D.D. No.: • Date: • Bank:		
RISL Processing Fee details	• Amount: • D.D. No.: • Date: • Bank:		
Bid Security (EMD) details	• Amount: • D.D./ BC/BG No.: • Date: • Bank:		
Legal Entity (Please tick mark)	Proprietorship firm/A company registered under Indian Companies Act, 1956/ A partnership firm registered under Indian Partnership Act, 1932		
Financial: Turnover from IT/ ITeS	Annual Turnover of the bidder from IT/ ITeS for (as per the published audited accounts): • 2020-21 • 2021-22 • 2022-23		
Technical Capability	• WO No.: • Issuing Agency: • WO Date: • WO Value: • Work Completion Certificate date: OR Invoice Date: • Type of work:		
Tax registration No.	• GST Registration No.: • PAN number.:		

ANNEXURE-4: BIDDER'S AUTHORIZATION CERTIFICATE{to be filled by the bidder}

To,
{Procuring entity},
_____,
_____,

I/ We {Name/ Designation} hereby declare/ certify that {Name/ Designation} is hereby authorized to sign relevant documents on behalf of the company/ firm in dealing with NIB reference No. _____ dated _____. He/ She is also authorized to attend meetings & submit technical & commercial information/ clarifications as may be required by you in the course of processing the Bid. For the purpose of validation, his/ her verified signatures are as under.

Thanking you,

Name of the Bidder: -
Authorised Signatory: -
Seal of the Organization: -
Date: _____
Place: _____

Verified Signature:

ANNEXURE-5: SELF-DECLARATION{to be filled by the bidder}

To,

{Procuring entity},

_____,

In response to the NIB Ref. No. _____ dated _____ for {Project Title}, as an Owner/ Partner/ Director/ Auth. Sign.of _____, I/ We hereby declare that presently our Company/ firm _____, at the time of bidding,: -

a) possess the necessary professional, technical, financial and managerial resources and competence required by the Bidding Document issued by the Procuring Entity;
b) have fulfilled my/ our obligation to pay such of the taxes payable to the Union and the State Government or any local authority as specified in the Bidding Document;
c) is having unblemished record and is not declared ineligible for corrupt & fraudulent practices either indefinitely or for a particular period of time by any State/ Central government/ PSU/ UT.
d) does not have any previous transgressions with any entity in India or any other country during the last three years
e) does not have any debarment by any other procuring entity
f) isnot insolvent in receivership, bankrupt or being wound up, not have its affairs administered by a court or a judicial officer, not have its business activities suspended and is not the subject of legal proceedings for any of the foregoing reasons;
g) does not have, and our directors and officers not have been convicted of any criminal offence related to their professional conduct or the making of false statements or misrepresentations as to their qualifications to enter into a procurement contract within a period of three years preceding the commencement of the procurement process, or not have been otherwise disqualified pursuant to debarment proceedings;
h) does not have a conflict of interest as mentioned in the bidding document which materially affects the fair competition.
i) will comply with the code of integrity as specified in the bidding document.

Also, this is to certify that, the specifications of goods which I/ We have mentioned in the Technical bid, and which I/ We shall supply if I/ We am/ are awarded with the work, are in conformity with the minimum technical specifications of the bidding document and that there are no deviations of any kind from the requirement specifications.

Also, I/ we have thoroughly read the bidding document and by signing this certificate, we hereby submit our token of unconditional acceptance to all the terms & conditions of the bidding document without any deviations and assumptions.

I/ We also certify that the price I/ we have quoted is inclusive of all the taxes to meet the desired Standards set out in the bidding Document.

I am/we are bonafide/ Manufacturers/ Whole Sellers/ Sole distributor/ Authorised dealer/ dealers/ sole selling/ Marketing agent in the goods/ stores/ equipment for which I/ We have quoted.

I/We have read the Rule 13 of RTPP Rules and Government of Rajasthan Notification No. F.2(1)FD/G&TSPFC/2017 dated 01.01.2021, 15.01.2021 and 30.03.2021 regarding Provisions for Procurement from a Bidder which shares a land border with India and I/we certify that,

I/we is/are not with beneficial ownership from such country and will not supplying finished goods procured directly or indirectly from such country.

OR

I/we is/are with beneficial ownership from such country and/or will be supplying finished goods procured directly or indirectly from such country and I/We are registered with the Competent Authority as specified in Rule 13 of RTPP Rules and Government of Rajasthan Notification No. F.2(1)FD/G&T-SPFC/2017 dated 01.01.2021, 15.01.2021 and 30.03.2021 and the evidence of valid registration with the Competent Authority is attached with the bid.

If this declaration is found to be incorrect then without prejudice to any other action that may be taken as per the provisions of the applicable Act and Rules thereto prescribed by GoR, my/ our security may be forfeited in full and our bid, to the extent accepted, may be cancelled.

Thanking you,

Name of the Bidder: -
Authorised Signatory: -
Seal of the Organization: -
Date: _____
Place: _____

ANNEXURE-6: MANUFACTURER'S AUTHORIZATION FORM (MAF){to be filled by the OEMs}

(Indicative Format)

To,
{Procuring Entity},
_____,

Subject: Issue of the Manufacturer's Authorisation Form (MAF)
Reference: NIB/ RFP Ref. No. _____ dated _____

Sir,
We {name and address of the OEM} who are established and reputed original equipment manufacturers (OEMs) having factories at {addresses of manufacturing location} do hereby authorize {M/s _____} who is our {Distributor/ Channel Partner/ Retailer/ Others <please specify>} to bid, negotiate and conclude the contract with you against the aforementioned reference for the following Hardware/ Software manufactured by us: -

{OEM will mention the details of all the proposed product(s) with their make/ model.}

We undertake to provide OEM Warranty for the offered Hardware/ Software, as mentioned above, for 3 Years.

We hereby confirm that the offered Hardware/ Software is not likely to be declared as End-of-Sale within next 12 months from the date of bid submission.

We hereby confirm that the offered Hardware/ Software is not likely to be declared as End-of-Service/ Support within next 5 years from the date of bid submission.]

Yours faithfully,
For and on behalf of M/s (Name of the manufacturer)

(Authorized Signatory)
Name, Designation & Contact No.:
Address: _____
Seal:

ANNEXURE-7: UNDERTAKING ON AUTHENTICITY OF COMPUTER EQUIPMENTS

{To be filled by the bidder(On Rs. 100/- Non-judicial stamp paper)}

To,
{Procuring Entity},
_____,

Reference: NIB No. : _____ Dated: _____

This has reference to the items being supplied/quoted to you vide bid ref. no. _____ dated _____.

We hereby undertake that all the components/parts/assembly/ software used in the equipment shall be genuine, original and new components /parts/assembly/software from respective OEMs of the products and that no refurbished/duplicate/ second hand components/ parts/ assembly/ software are being used or shall be used. In respect of licensed operating system, we undertake that the same shall be supplied along with the authorized license certificate with our name/logo. Also, that it shall be sourced from the authorized source for use in India.

In case, we are found not complying with above at the time of delivery or during installation, for the equipment already billed, we agree to take back the equipment already supplied at our cost and return any amount paid to us by you in this regard and that you will have the right to forfeit our Bid Security/ SD/ PSD for this bid or debar/ black list us or take suitable action against us.

Authorized Signatory
Name:
Designation:

ANNEXURE-8: COMPONENTS OFFERED – BOM{to be filled by the bidder}

Please fill the following BOM for all the offered components.

Sl. No.	Product Details (Only one make and model)	OEM Part Code (OEM Part code Datasheet shall be enclosed in the bid)	Detailed Technical Specification Reference**	OEM Details (Name: Address: E-Mail: Mobile No.:)
			{Item No. xx} {Item No. xx} {Item No. xx} {Item No. xx}	

**** Please attach technical specifications compliance sheet (only on OEM's letter-head / OEM email as specified in Annexure-2) and provide reference number in this column. (Deviations, if any, should be appropriately mentioned & highlighted in the compliance/ deviation column of the respective table as provided in Annexure-2: Technical Specifications of this bidding document)**

ANNEXURE-9: FINANCIAL BID COVER LETTER & FORMAT

COVER LETTER {to be submitted by the bidder on his Letter head}

To,
The Managing Director,
RajCOMP Info Services Limited (RISL),
First Floor, YojanaBhawan, C-Block, Tilak Marg, C-Scheme, Jaipur-302005 (Raj).

Reference: NIB No. :_____ Dated:_____

Dear Sir,

We, the undersigned bidder, Having read & examined in detail, the Bidding Document, the receipt of which is hereby duly acknowledged, I/ we, the undersigned, offer to supply/ work as mentioned in the Scope of the work, Bill of Material, Technical specifications, Service Level Standards & in conformity with the said bidding document for the same.

I / We undertake that the prices are in conformity with the specifications prescribed. The quote/ price are inclusive of all cost likely to be incurred for executing this work. The prices are inclusive of all type of govt. taxes/duties as mentioned in the financial bid (BoQ).

I / We undertake, if our bid is accepted, to deliver the goods in accordance with the delivery schedule specified in the schedule of Requirements.

I/ We hereby declare that in case the contract is awarded to us, we shall submit the contract performance guarantee as prescribed in the bidding document.

I / We agree to abide by this bid for a period of _____ days after the last date fixed for bid submission and it shall remain binding upon us and may be accepted at any time before the expiry of that period.

Until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and your notification of award shall constitute a binding Contract between us.

I/ We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We understand that you are not bound to accept the lowest or any bid you may receive.
We agree to all the terms & conditions as mentioned in the bidding document and submit that we have not submitted any deviations in this regard.

Date:
Authorized Signatory
Name:
Designation:

Financial Bid Format (BoQ1):-Equipment/Appliance including three years subscription & comprehensive onsite OEM Warranty & premium support (CAPEX)

{to be submitted by the bidder only in BoQ format (.XLS) available at e-Procurement portal}

Sr. No	Name of Item	Qty	Unit Rate including all taxes, Govt. levies and duties but except GST	Applicable GST' (in Rs.) on Col-4	Unit Rate including all taxes & GST (in Rs.)	Total Amount inclusive of all taxes, levies and GST
1	2	3	4	5	6=4+5	7 = 6 x 3
1.	Security Orchestration, Automation & Response (SOAR) Solution with Threat Intelligence Platform (TIP) - DC	01				
2.	Incident Response Solution/Services - DC	01				
3.	Unified Threat Intelligence Platform (UIP) - DC	01				
4.	Network Behavior Anomaly Detection (NBAD)/NDR - DC	01				
5.	DNS Security - DC	01				
6.	Anti-Advanced Persistent Threats solution (APT) - DC	01				
7.	SIEM with UEBA - DC	01				
8.	Network forensic (Packet Capture and Re-Construction Capability) - DC	01				
9.	Network forensic (Packet Capture and Re-Construction Capability) – DC (SecLAN)	01				
10.	WAF with API Security - DC	01				
11.	Database Access Management (DAM) - DC	01				
12.	Anti-Advanced Persistent Threats solution (APT) – DR	01				

13.	WAF with API Security– DR	01				
14.	Network forensic (Packet Capture and Re-Construction Capability) – DR	01				
Total Amount (In Figures):						
Total Amount (In Words):						

Financial Bid Format (BoQ2):- Manpower BoQ

{to be submitted by the bidder only in BoQ format (.XLS) available at e-Procurement portal}

Sr. No	Name of Item	Qty (Man-Month)	Unit Man-Month Rate including all taxes, Govt. levies and duties but except GST	Applicable GST (in Rs.) on Col-4	Unit Rate including all taxes & GST (in Rs.)	Total Amount inclusive of all taxes, levies and GST (OPEX)
1	2	3	4	5	6=4+5	7 = 6 x 3
1.	Analyst(Tier-1)	12 X 36 = 432				
2.	Analyst(Tier-2)	6 X 36 = 216				
3.	Analyst(Tier-3)	3 X 36 = 108				
4.	Threat Hunter-L2	2 X 36 = 72				
5.	Forensic Analyst - L2	1 X 36 = 36				
6.	Risk & Compliance Auditor - L2	1 X 36 = 36				
7.	SOC Manager	1 X 36 = 36				
8.	OEM certified Resources – SIEM - L2	1 X 36 = 36				
9.	OEM certified Resources – SOAR - L2	1 X 36 = 36				
10.	OEM certified Resources - WAF- L2	1 X 36 = 36				
11.	OEM certified Resources - NBAD- L2	1 X 36 = 36				
Total Amount (In Figures):						
Total Amount (In Words):						

Financial Bid Format (BoQ3):- Summary BoQ

{to be submitted by the bidder only in BoQ format (.XLS) available at e-Procurement portal}

Sr. No	Name of Item	Qty	Total Amount inclusive of all taxes, levies and GST
1	2	3	4
1.	**Total of (BoQ1): Equipment/Appliance including three years subscription & comprehensive onsite OEM Warranty & premium support**	01	
2.	Total of (BoQ2): Manpower BoQ	01	
Total Amount (In Figures):			
Total Amount (In Words):			

NOTE:

a. GST rate should be as per prevailing rates.
b. The L1 bidder shall evaluated on the sum of Row "**Total Amount**" (Column-7) of above BoQ (BoQ3- Summary BoQ).
c. Bidders are expected to quote for all the item categories mentioned in above table. In case a bidder does not quote for any of the item category, the bid shall be summarily rejected.
d. In case of any descripencicy found in above BoQ (BoQ3) and respective BoQ (BoQ1 and BoQ2) than the rates filled in respective BoQ (BoQ1 and BoQ2) shall be prevail and L1 bidder shall be evaluated accordingly.
e. In case a bidder fails to indicate the amount of GST, in the prescribed column then the bid value shall be calculated without including the component of GST for the purpose of bid evaluation, and total bid price shall be consipaydered accordingly.
f. The bidder has to ensure that their Price bid contains reasonable unit rates of CAPEX and OPEX items. Authority may identify abnormally higher / lower unit rates of line items and seek justifications from bidders on the same.

ANNEXURE-10: BANK GUARANTEE FORMAT {to be submitted by the bidder's bank only if bank guarantee submission is allowed in this bidding document}

BANK GUARANTEE FORMAT – BID SECURITY

(To be stamped in accordance with Stamp Act and to be issued by a Nationalised/ Scheduled bank having its branch at Jaipur and payable at par at Jaipur, Rajasthan)

The Managing Director,
RajCOMP Info Services Limited (RISL),
First Floor, YojanaBhawan, C-Block, Tilak Marg, C-Scheme, Jaipur-302005 (Raj).

Sir,

1. In accordance with your Notice Inviting Bid for <please specify the project title> vide NIB reference no. <please specify> M/s. …….. (Name & full address of the firm) (Hereinafter called the "Bidder") hereby submits the Bank Guarantee to participate in the said procurement/ bidding process as mentioned in the bidding document.

   It is a condition in the bidding documents that the Bidder has to deposit Bid Security amounting to <Rs. _____ (Rupees <in words>)> in respect to the NIB Ref. No. _____ dated _____ issued by RISL, First Floor, Yojana Bhawan, C-Block, Tilak Marg, C-Scheme, Jaipur, Rajasthan (hereinafter referred to as "RISL") by a Bank Guarantee from a Nationalised Bank/ Scheduled Commercial Bank having its branch at Jaipur irrevocable and operative till the bid validity date (i.e. <please specify> days from the date of submission of bid). It may be extended if required in concurrence with the bid validity.

   And whereas the Bidder desires to furnish a Bank Guarantee for a sum of <Rs. _____ (Rupees <in words>)> to the RISL as earnest money deposit.

2. Now, therefore, we the ……..…… (Bank), a body corporate constituted under the Banking Companies (Acquisition and Transfer of Undertaking) Act. 1969 (delete, if not applicable) and branch Office at…….... (Hereinafter referred to as the Guarantor) do hereby undertake and agree to pay forthwith on demand in writing by the RISL of the said guaranteed amount without any demur, reservation or recourse.

3. We, the aforesaid bank, further agree that the RISL shall be the sole judge of and as to whether the Bidder has committed any breach or breaches of any of the terms costs, charges and expenses caused to or suffered by or that may be caused to or suffered by the RISL on account thereof to the extent of the Earnest Money required to be deposited by the Bidder in respect of the said bidding document and the decision of the RISL that the Bidder has committed such breach or breaches and as to the amount or amounts of loss, damage, costs,

charges and expenses caused to or suffered by or that may be caused to or suffered by the RISL shall be final and binding on us.

4. We, the said Bank further agree that the Guarantee herein contained shall remain in full force and effect until it is released by the RISL and it is further declared that it shall not be necessary for the RISL to proceed against the Bidder before proceeding against the Bank and the Guarantee herein contained shall be invoked against the Bank, notwithstanding any security which the RISL may have obtained or shall be obtained from the Bidder at any time when proceedings are taken against the Bank for whatever amount that may be outstanding or unrealized under the Guarantee.

5. Any notice by way of demand or otherwise hereunder may be sent by special courier, telex, fax, registered post or other electronic media to our address, as aforesaid and if sent by post, it shall be deemed to have been given to us after the expiry of 48 hours when the same has been posted.

6. If it is necessary to extend this guarantee on account of any reason whatsoever, we undertake to extend the period of this guarantee on the request of our constituent under intimation to you.

7. The right of the RISL to recover the said amount of <Rs. _____ (Rupees <in words>)> from us in manner aforesaid will not be precluded/ affected, even if, disputes have been raised by the said M/s. ……(Bidder) and/ or dispute or disputes are pending before any court, authority, officer, tribunal, arbitrator(s) etc.

8. Notwithstanding anything stated above, our liability under this guarantee shall be restricted to <Rs. _____ (Rupees <in words>)> and our guarantee shall remain in force till bid validity period i.e. <please specify> days from the last date of bid submission and unless a demand or claim under the guarantee is made on us in writing within three months after the Bid validity date, all your rights under the guarantee shall be forfeited and we shall be relieved and discharged from all liability thereunder.

9. This guarantee shall be governed by and construed in accordance with the Indian Laws and we hereby submit to the exclusive jurisdiction of courts of Justice in India for the purpose of any suit or action or other proceedings arising out of this guarantee or the subject matter hereof brought by you may not be enforced in or by such count.

10. We hereby confirm that we have the power/s to issue this Guarantee in your favor under the Memorandum and Articles of Association/ Constitution of our bank and the undersigned is/are the recipient of authority by express delegation of power/s and has/have full power/s to execute this guarantee under the Power of Attorney issued by the bank in your favour.

Date …… (Signature) …….

Place …… (Printed Name) …….
(Designation) ……
(Bank's common seal) …….

In presence of:
WTTNESS (with full name, designation, address & official seal, if any)
(1) ……
……
(2) ……
……

Bank Details
Name & address of Bank:
Name of contact person of Bank:
Contact telephone number:

GUIDELINES FOR SUBMISSION OF BANK GUARANTEE

The Bank Guarantee shall fulfil the following conditions in the absence of which they cannot be considered valid: -

1. Bank Guarantee shall be executed on non- judicial stamp paper of applicable value purchased in the name of the bank.
2. Two persons should sign as witnesses mentioning their full name, designation, address and office seal (if any).
3. The Executor (Bank Authorities) may mention the power of attorney No. and date of execution in his/ her favour authorizing him/ her to sign the document. The Power of Attorney to be witnessed by two persons mentioning their full name and address.
4. The Bank Guarantee should be executed by a Nationalised Bank/ Scheduled Commercial Bank only.
5. Non – Judicial stamp paper shall be used within 6 months from the date of Purchase of the same. Bank Guarantee executed on the non-judicial stamp paper after 6 (six) months of the purchase of such stamp paper shall be treated as non-valid.
6. The contents of Bank Guarantee shall be strictly as per format prescribed by RISL
7. Each page of Bank Guarantee shall bear signature and seal of the Bank and B.G. number.
8. All corrections, deletions etc. in the Bank Guarantee should be authenticated by signature of Bank Officials signing the Bank Guarantee.
9. Non-judicial stamp paper (Rajasthan only) with stamp duty of 0.25% of the BG value or 25,000 whichever is lower.
10. Bank should separately send through registered post/courier a certified copy of Bank Guarantee, mentioning Bid reference, Bid title and bidder name, directly to the RISL at the following address:

BANK GUARANTEE FORMAT – PERFORMANCE SECURITY (PBG)

(To be stamped in accordance with Stamp Act and on a Stamp Paper purchased from Rajasthan State only and to be issued by a Nationalised/ Scheduled bank having its branch at Jaipur and payable at par at Jaipur, Rajasthan)

To,
The Managing Director,
RajCOMP Info Services Limited (RISL),
First Floor, YojanaBhawan, C-Block, Tilak Marg, C-Scheme, Jaipur-302005 (Raj).

1. In consideration of the RajCOMP Info Services Limited (hereinafter called "RISL") having agreed to exempt M/s .....(hereinafter called "the said Contractor(s)" from the demand, under the terms and conditions of an Agreement No.....dated .....made between the RISL through …… and .....(Contractor) for the work .....(hereinafter called "the said Agreement") of Security Deposit for the due fulfilment by the said Contractor (s) of the terms and conditions contained in the said Agreement, on production of a Bank Guarantee for Rs.....(rupees .....only), we .....(indicate the name of the Bank), (hereinafter referred to as "the Bank") at the request of .....Contractor(s) do hereby undertake to pay to the RISL an amount not exceeding Rs.....(Rupees.....only) on demand.
2. We..... (Indicate the name of Bank), do hereby undertake to pay Rs..... (Rupees.....only), the amounts due and payable under this guarantee without any demur or delay, merely on a demand from the RISL. Any such demand made on the bank by the RISL shall be conclusive as regards the amount due and payable by the Bank under this guarantee. The Bank Guarantee shall be completely at the disposal of the RISL and We..... (Indicate the name of Bank), bound ourselves with all directions given by RISL regarding this Bank Guarantee. However, our liability under this guarantee shall be restricted to an amount not exceeding Rs..... (Rupees.....only).
3. We.....(indicate the name of Bank), undertake to pay to the RISL any money so demanded notwithstanding any dispute or disputes raised by the contractor(s) in any suit or proceeding pending before any Court or Tribunal or Arbitrator etc. relating thereto, our liability under these presents being absolute, unequivocal and unconditional.
4. We.....(indicate the name of Bank) further agree that the performance guarantee herein contained shall remain in full force and effective up to <DATE> and that it shall continue to be enforceable for above specified period till all the dues of RISL under or by virtue of the said Agreement have been fully paid and its claims satisfied or discharged or till the RISL certifies that the terms and conditions of the said Agreement have been fully and properly carried out by the said Contractor(s) and accordingly discharges this guarantee.
5. We .....(indicate the name of Bank) further agree with the RISL that the RISL shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said Agreement or to extend time of performance by the said Contractor(s) from time to time or to postpone for

any time or from time to time any of the powers exercisable by the RISL against the said Contractor(s) and to forbear or enforce any of the terms and conditions relating to the said Agreement and we shall not be relieved from our liability by reason of any such variation, or extension being granted to the said Contractor(s) or for any forbearance, act or omission on the part of the RISL or any indulgence by the RISL to the said Contractor(s) or by any such matter or thing whatsoever which would but for this provision, have effect of so relieving us.

6. The liability of us ..... (indicate the name of Bank), under this guarantee will not be discharged due to the change in the constitution of the Bank or the contractor(s).
7. We ..... (indicate the name of Bank), lastly undertake not to revoke this guarantee except with the previous consent of the RISL in writing.
8. This performance Guarantee shall remain valid and in full effect, until it is decided to be discharged by the RISL. Notwithstanding anything mentioned above, our liability against this guarantee is restricted to Rs..... (Rupees.....only).
9. It shall not be necessary for the RISL to proceed against the contractor before proceeding against the Bank and the guarantee herein contained shall be enforceable against the Bank notwithstanding any security which the RISL may have obtained or obtain from the contractor.
10. We ..... (indicate the name of Bank) verify that we have a branch at Jaipur. We undertake that this Bank Guarantee shall be payable at any of its branch at Jaipur. If the last day of expiry of Bank Guarantee happens to be a holiday of the Bank, the Bank Guarantee shall expire on the close of the next working day.
11. We hereby confirm that we have the power(s) to issue this guarantee in your favor under the memorandum and articles of Association/constitution of our bank and the undersigned is/are the recipient of authority by express delegation of power(s) and has/have full power(s) to execute this guarantee for the power of attorney issued by the bank.

Dated.....day of.....For and on behalf of the <Bank> (indicate the Bank)

Signature
(Name & Designation)
Bank's Seal

The above performance Guarantee is accepted by the RISL
For and on behalf of the RISL

Signature

(Name & Designation)

ANNEXURE-11: DRAFT AGREEMENT FORMAT{to be mutually signed by selected bidder and procuring entity}

This Contract is made and entered into on this _____day of _____, 2024 by and between RajCOMP Info Services Limited (RISL), having its head office at First Floor, Yojana Bhawan, Tilak Marg, C-Scheme, Jaipur-302005, Rajasthan (herein after referred to as Purchaser/ RISL) which term or expression, unless excluded by or repugnant to the subject or context, shall include his successors in office and assignees on ONE PART

And
M/s_____, a company registered under the Indian Companies Act, 1956 with its registered office at _____ (herein after referred as the "Successful Bidder/ Supplier") which term or expression, unless excluded by or repugnant to the subject or context, shall include his successors in office and assignees on the OTHER PART.

Whereas,
Purchaser is desirous of appointing an agency for <project title>as per the Scope of Work and Terms and Conditions as set forth in the RFP document dated _____ of <NIB No _____>.

And whereas
M/s_____ represents that it has the necessary experience for carrying out the overall work as referred to herein and has submitted a bid and subsequent clarifications for providing the required services against said NIB and RFP document issued in this regard, in accordance with the terms and conditions set forth herein and any other reasonable requirements of the Purchaser from time to time.

And whereas
Purchaser has accepted the bid of supplier and has placed the Work Order / Letter of Intent vide Letter No. _____dated_____, on which supplier has given their acceptance vide their Letter No._____dated _____.

And whereas
The supplier has deposited a sum of Rs. _____/- (Rupees _____) in the form of _____ ref no. _____ dated _____ of _____ Bank and valid up to _____ as security deposit for the due performance of the contract.

Now it is hereby agreed to by and between both the parties as under:

1. The NIB Ref. No. .....and RFQ i.e. Final RFQ document issued by RISL along with its enclosures/ Annexures, wherever applicable, are deemed to be taken as part of this contract and are binding on both the parties executing this contract.
2. In consideration of the payment to be made by the RISL to the Successful Bidder at the rates set forth in the Work Order No. _____dated _____, the Successful Bidder will duly provide the related services in the manner set forth in the RFQ, along with its enclosures/ annexures along with subsequent clarifications submitted by the Successful Bidder.
3. The RISL do hereby agrees that if the Successful Bidder shall duly provide related services in the manner aforesaid observe and keep the said terms and conditions of the RFQ and Contract, the purchaser will pay or cause to be paid to the Successful Bidder, at the time and the manner set forth in the said conditions of the RFQ, the amount payable for each and every milestone & deliverable. The mode of Payment will be as specified in the RFQ document.
4. The timelines for the prescribed Scope of Work shall be effective from the date of Work Order and completed by the Successful Bidder within the period as specified in the RFQ document.
5. In case of extension in the delivery period and/or completion period is granted with liquidated damages, the recovery shall be made on the basis of following percentages of value of Goods and Services which the selected bidder has failed to supply or complete the work:-

Sr.	Condition	LD %*
a.	Delay up to one fourth period of the prescribed delivery period & completion of Goods and Services.	2.5 %
b.	Delay exceeding one fourth but not exceeding half of the prescribed delivery period & completion of Goods and Services.	5.0 %
c.	Delay exceeding half but not exceeding three fourth of the prescribed delivery period & completion of Goods and Services.	7.5 %
d.	Delay exceeding three fourth of the prescribed delivery period, & completion of Goods and Services.	10.0 %

Note:

i. Fraction of a day in reckoning period of delay in services shall be eliminated if it is less than half a day.
ii. The maximum amount of agreed liquidated damages shall be 10%. The percentage refers to the payment due for the associated milestone.
iii. If the Successful Bidder requires an extension of time in completion of services on account of occurrence of any hindrances, he shall apply in writing to the authority which had placed the work order, for the same immediately on occurrence of the hindrance but not after the stipulated date of completion of services and it shall be discretion of the authority to extend the same or not.
iv. Delivery completion period may be extended with or without liquidated damages on the will of authority if the delay in the service/ delivery in on account of hindrances beyond the control of the Successful Bidder.

6. The Penalties shall be implemented and deducted as per the SLAs defined in the RFP.

7. All disputes arising out of this agreement and all questions relating to the interpretation of this agreement shall be decided as per the procedure mentioned in the RFQ document.
8. In case of agreement with Supplier/service provider:
   "This agreement is being executed on behalf of M/s (Concerned Department) ……., to procure defined goods and services, RISL is acting merely as a Pure Agent who neither intends to hold or holds any title to the goods and services being procured or provided. So all the goods and services are required to be delivered in the name of M/s (Concerned Department) ……. along with invoices of supplied items, although payment will be made by RISL on behalf of said department/company."
9. In case of MOU with Department/PSU
   "This MOU is being executed to procure defined goods and services, RISL is acting merely as a Pure Agent who neither intends to hold or holds any title to the goods and services being procured or provided. So all the goods and services (except management consultancy) will be delivered in the name of M/s (Concerned Department)……. along with invoices of supplied items, although payment will be made by RISL on behalf of M/s (Concerned Department)……."

In witness whereof the parties hereto have set their hands on the _____ day of_____ (Year).

Signed By:	Signed By:
( ) Designation: Company:	( ) Designation: RajCOMP Info Services Limited, Jaipur
In the presence of:	In the presence of:
( ) Designation: Company:	( ) Designation: RajCOMP Info Services Limited, Jaipur
( ) Designation: Company:	( ) Designation: RajCOMP Info Services Limited, Jaipur

ANNEXURE-12: MEMORANDUM OF APPEAL UNDER THE RTPP ACT, 2012

Appeal No ……of ……
Before the …… (First/ Second Appellate Authority)

1. Particulars of appellant:
    a. Name of the appellant: <please specify>
    b. Official address, if any: <please specify>
    c. Residential address: <please specify>

2. Name and address of the respondent(s):
    a. <please specify>
    b. <please specify>
    c. <please specify>

3. Number and date of the order appealed against and name and designation of the officer/ authority who passed the order (enclose copy), or a statement of a decision, action or omission of the procuring entity in contravention to the provisions of the Act by which the appellant is aggrieved:<please specify>

4. If the Appellant proposes to be represented by a representative, the name and postal address of the representative:<please specify>

5. Number of affidavits and documents enclosed with the appeal:<please specify>

6. Grounds of appeal (supported by an affidavit):<please specify>

7. Prayer:<please specify>

Place …….

Date ……

Appellant's Signature

ANNEXURE-13: PRE-BID QUERIES FORMAT {to be filled by the bidder}

Name of the Company/Firm: _____

_____

_____

Bidding Document Fee Receipt No. _____ Dated_____ for Rs. _____/-

Name of Person(s) Representing the Company/ Firm:

Name of Person	Designation	Email-ID(s)	Tel. Nos. & Fax Nos.

Company/Firm Contacts:

Contact Person(s)	Address for Correspondence	Email-ID(s)	Tel. Nos. & Fax Nos.

Query / Clarification Sought:

S.No.	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification

Note: - Queries must be strictly submitted only in the prescribed format (.XLS/ .XLSX/ .ODF). Queries not submitted in the prescribed format and without receipt of tender document fee will not be considered/ responded at all by the procuring entity. Also, kindly attach the coloured scanned copy of the receipt towards the submission of the bidding/ tender document fee.

ANNEXURE-14: FORM OF BID-SECURING DECLARATION

{To be filled by the Govt./PSU/Department only as per RFP}
(Required to be submit with technical bid and in physical as mentioned in NIB)

To,
The Commissioner,
Department of Information Technology & Communication (DOIT&C),
IT Building, Yojana Bhawan, C-Block,
Tilak Marg, C-Scheme, Jaipur-302005 (Raj).

I/ We {Name of the PSU/Corporation/Department} hereby {Name of the PSU/Corporation/Department} is owned or controlled or managed by the {Name of the State} State Government/Central Government Undertaking/Department. I/ We hereby declare/ certify that it is eligible for exemption from the bid security submission as per RFP.

Legal document/Certificate of Incorporation establishing the exemption is attached.
Thanking you,

Name of the Bidder:
Name of Authorised Signatory:
Sign of the Authorised Signatory
Seal of the Organization: -
Date:
Place:

ANNEXURE-15: INDICATIVE CONFIDENTIALITY AND NON DISCLOSURE AGREEMENT

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

This confidentiality and non-disclosure agreement ("Agreement") is made on this _____day of ____, (Year)

BETWEEN

Managing Director, RajComp Info Services Ltd., B-Block, 1st Floor, Yojna Bhawan, Tilak Marg, C-Scheme, Jaipur-302005 (hereinafter referred to as "RISL", which expression shall, unless repugnant to the context hereof or excluded specifically, mean and include its successors, assigns and administrators) of the FIRST PART,

AND

Company Name, India (hereinafter referred to as **'**Successful Bidder/ Supplier**'**, which expression shall, unless repugnant to the context hereof or excluded specifically, mean and include its successors, assigns and administrators) of the SECOND PART.

WHEREAS

a. The RISL wishes to appoint an agency for_____Yojana Bhawan, Jaipur for a period of __ years. For the purpose there will be a requirement to exchange certain information related to or hosted in Rajasthan State Data Centre (RSDC) which is proprietary and confidential information.
b. The RISL is willing to disclose such information to successful bidder only on the terms and conditions contained in this Agreement. The successful bidder agrees to hold the Covered Data and Information in strict confidence. Successful bidder shall not use or disclose Covered Data and Information received from or on behalf of Government of Rajasthan/RISL except as permitted or required by the Agreement, or as otherwise authorized in writing by RISL.

NOW, THEREFORE, THE PARTIES HERETO AGREE AS FOLLOWS:

1. **Definition: In this agreement unless the contest otherwise requires:**

1.1. "Confidential Information" shall mean

a) any and all information concerning Rajasthan State Data Centre (RSDC)or any other successor,
b) any and all trade secrets or other confidential or proprietary information related and hosted in State Data Centre (SDC)
c) Passwords of IT/Non IT equipments of SDC, user identifications, or other information that may be used to access information systems, networking diagrams, technical specifications of IT/Non IT equipments, policies of firewall/IDs/IPS

/routers /switches and information hosted on IT equipments in Rajasthan State Data Centre (RSDC)

1.2. Proprietary Information shall mean as technical data and other information (including but not limited to digital data, products, substances, organisms, technology, research results or plans, system processes, workflows, know-how, reports, descriptions, drawings, design, compositions, strategies, trade secrets, business and financial information, and computer software) in whatever form, which is related or hosted with Rajasthan State Data Centre (RSDC)and is disclosed or delivered by the First Party to the Second Party, whether by means of written or oral disclosure or otherwise.

2. **Limitations on Use and Disclosure of Confidential and Proprietary Information**

2.1. Confidential and Proprietary Information disclosed by the RISL and/or other departments/PSU whose data are hosted in Rajasthan State Data Centre (RSDC)shall be used by the successful bidder solely for the purpose of fulfillment of the obligation and work assigned to it as per order no._____and shall not otherwise be used for his benefit or otherwise. All information encountered in the performance of duties shall be treated as confidential unless and until advised otherwise by RISL or its representative. Successful bidder shall not share, record, transmit, alter, or delete information residing/hosted in the information systems except as required in performance of the job duties.

2.2. Confidential and Proprietary Information shall not be copied or reproduced by the successful BIDDER without the express written permission of the RISL, except for such copies as may be reasonably required for accomplishment of the purpose stated in the tender no._____.

2.3. Confidential and Proprietary Information shall be disclosed only to the Director or employees of the successful bidder who have a 'need to know' in connection with the purpose stated above, and who additionally agree to the nondisclosure requirements of this Agreement. Any further disclosure of confidential and Proprietary Information by the successful bidder shall be treated as a breach of this Agreement by the successful bidder.

2.4. Confidential and Proprietary Information shall not be disclosed by the successful bidder to any third party without the prior written consent of the First Party.

2.5. This Agreement shall not restrict disclosure or use of Confidential and Proprietary Information which:

a. was in the public domain at the time of disclosure or thereafter enters the public domain through no breach of this Agreement by the successful bidder; or
b. was, at the time of receipt, otherwise known to the successful bidder without restriction as to use or disclosure; or

c. becomes known to the successful bidder from a source other than the RISL and/or other departments/PSU without a breach of this Agreement by the successful bidder; or
d. is developed independently by the successful bidder without the use of Proprietary Information disclosed to it hereunder; or
e. is otherwise required to be disclosed by law.

3. Business Obligation:

3.1. During the complete contract period and even after 3 years of the expiry of the agreement, the successful bidder shall not
   a. Disclose Confidential Information in any manner or form to any person other than its own employees for the limited purpose stated herein, or
   b. Use Confidential Information for its own benefit or for the benefit of any person or entity other than the RISL, without the prior written consent of the RISL .

3.2. Whereas, the RISL as a matter of policy and with a view to operate and maintain SDC has given order to the successful bidder Work Order Nofor _____at Yojana Bhawan, Jaipur for a period of __ year as specified in the service level agreement (SLA).

3.3. Whereas, the RISL under the circumstances referred, herein before, wants to protect itself from any misuse of the confidential and proprietary information by the third party i.e. person or persons (employees of successful bidder), had entered into an agreement with the successful BIDDER that the second party shall not divulge such information either during the course of the life of this agreement or even after the expiry of the agreement.

3.4. Whereas, the successful bidder has agreed to fully abide by the terms of this non-disclosure agreement and it has also been agreed by the parties that if there will be any breach or violation of the terms of agreement vis-à-vis non-disclosure clause, the successful bidder shall not only be liable for consequential costs and damages but in addition to that will also be liable for criminal prosecution in accordance with the prevailing laws.

3.5. whereas, the successful bidder having in his possession or control any secret official code or password or digital data or any sketch, plan, model, article, note, document or information which falls within the purview of confidential or proprietary information, the successful bidder shall not part with any part of such information to anyone under any circumstances, whatsoever, without the prior approval of the risl and if this is violated, the risl shall have the legal right to initiate civil and criminal proceeding against it under the provisions of the relevant law.

3.6. Whereas, the RISL shall have the entire control over the functioning of the Successful

bidder and the successful bidder shall work according to the instruction of the RISL and in case if this is violated by the successful bidder in any mode or manner, the RISL shall have the legal right to initiate civil and criminal proceeding against it under the provisions of the relevant law.

3.7. Whereas, if the successful bidder permits any person or persons without permission of the RISL to have –

a. Access or secures access to such computer, computer system or computer network which has the connectivity with the confidential and proprietary information or;
b. Downloads, copies or extracts any data, computer data base or information from such Database Server, Web Server, Computer System, networking equipments or Computer Network including information or data held or stored in any removable storage medium which has the connectivity with the confidential and proprietary information or;
c. Damages any Database Server or causes to damage any Database Server, Web Server, computer system, computer network, data, data base or any other programmes residing in such Server, computer system or computer network;
d. Denies or causes the denial of access to any authorized person of the RISL to have access to any computer system or computer network by any means;

Shall be liable to pay damages by way of compensation and would also be liable for criminal prosecution in accordance with the prevailing laws.

3.8 successful bidder shall report to RISL any use or disclosure of confidential and/or proprietary information/data not authorized by this Agreement in writing by RISL. Successful bidder shall make the report to RISL within not less than one (1) business day after successful bidder learns of such use or disclosure. Successful bidder's report shall identify:

a) The nature of the unauthorized use or disclosure,
b) The confidential and/or proprietary information/data used or disclosed,
c) Who made the unauthorized use or received the unauthorized disclosure,
d) What successful bidder has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and
e) What corrective action successful bidder has taken or shall take to prevent future similar unauthorized use or disclosure.

SUCCESSFUL BIDDER shall provide such other information, including a written report, as reasonably requested by RISL.

3.9 The successful bidder hereby agrees and consents that temporary or permanent injunctive relief and/or an order of specific performance may be granted in lieu of, or in addition to other available relief in any proceeding brought by RISL to enforce this Agreement, without the necessity of proof of actual damages and without posting bond for such relief.

4. **Dispute Resolution:**

4.1. Whereas, both the parties have agreed that in the event of any dispute or differences arising in between the parties, the courts at Jaipur shall only have jurisdiction to adjudicate the disputes/differences.

IN WITNESS WHERE OF the Parties here to have hereunto set their hands and seal the day and year first above written.

Signed By:	Signed By:
( ) Designation:, Company:	Managing Director, RISL
In the presence of:	*In the presence of:*
( ) Designation: Company:	() Designation: RISL
( ) Designation: Company:	() Designation:

ANNEXURE-16: TECHNICAL MANPOWER DETAILS

A) Minimum Educational Qualification & Experience Required

SN	Resource Type	Min. Edu. Qualification and Experience
1.	Analyst (Tier-1)	B.E./ B.Tech/ MCA/ M.Sc. in Computer Science or IT with 2+ years of relevant experience Certifications: CEH
2.	Analyst (Tier-2)	B.E./ B.Tech/ MCA/ M.Sc. in Computer Science or IT with 3+ years of relevant experience Certifications: CEH
3.	Analyst (Tier-3)	B.E./ B.Tech/ MCA/ M.Sc. in Computer Science or IT with 5+ years of relevant experience
4.	Threat Hunter – L3 Regular Day Shift	B.E./ B.Tech/ MCA/ M.Sc. in Computer Science or IT with 5+ years of relevant experience Certifications: CEH/CSA
5.	Risk & Compliance- L3 Auditor Regular Day Shift	B.E./ B.Tech in IT/CS/ECE with 8+ years of relevant experience. Should have any valid auditing certification.
6.	SOC Manager Regular Day Shift	B.E./ B.Tech/ MCA/ M.Sc. in Computer Science + or IT with 10+ years of relevant experience. Certifications: CISSP/CISM
7.	Forensic Analyst - L2 Regular Day Shift	B.E./ B.Tech/ MCA/ M.Sc. in Computer Science + with 3+ years of relevant experience. Certifications: CHFI
8.	OEM certified Resources - SIEM- L2 Regular Day Shift	B.E./ B.Tech in IT/CS/ECE or MCA/ M.Sc. in Computer Science or IT with 3+ years of relevant experience. Certifications: Proposed OEM Level Certification
9.	OEM certified Resources - SOAR - L2 Regular Day Shift	B.E./ B.Tech in IT/CS/ECE or MCA/ M.Sc. in Computer Science or IT with 3+ years of relevant experience. Certifications: Proposed OEM Level Certification
10.	OEM certified Resources - WAF- L2 Regular Day Shift	B.E./ B.Tech in IT/CS/ECE or MCA/ M.Sc. in Computer Science or IT with 3+ years of relevant experience. Certifications: Proposed OEM Level Certification
11.	OEM certified Resources – NBAD/Network Forensic - L2 Regular Day Shift	B.E./ B.Tech in IT/CS/ECE or MCA/ M.Sc. in Computer Science or IT with 3+ years of relevant experience. Certifications: Proposed OEM Level Certification

B) Job Description (As guided by the Project In-charge and as following but not limited to):

SN	Manpower/ Analyst/ Resource Type	Job Description
1.	Analyst (Tier-1)	• Real-time monitoring of all security appliance(s) like Secure Web/ Email Gateways, Proxy, IPS/ IDS, NGFW, DLP, APT, WAF, Network Forensics, SIEM, NAC, SOAR, etc. in RSDC for security events. • Endpoint Threat Detection • Reporting the security events/ incidents to Tier-2 and other relevant/ designated stakeholders (RSDC/ SecLAN/ RajSWAN/ RajNET/ RajWiFi/ NIC etc. FMS Teams etc.) • Communicating Emergency Alerts & Warnings to relevant/ designated stakeholders
2.	Analyst (Tier-2)	• Incident Analysis • Incident co-ordination & Response • Remote Incident Response • Forensics Artifact handling & Analysis • Malware Analysis • Insider Threat Case Support • Sensor Tuning & Maintenance • Custom Signature/ Rules Creation • Scripting & Automation • Audit Collection & Storage • Product Assessment & Deployment • Risk Assessment • Response Planning • Mitigation • Recovery Planning • Communicating Emergency Alerts & Warnings to relevant/ designated stakeholders
3.	Analyst (Tier-3)	• Cyber News Collection & Analysis, Distribution, Creation, Fusion • Local/ Global Threat Feed Tools • Security Trends • SOC Automation • Forensics Artifact handling & Analysis • Incident Response • Tradecraft Analysis • Security Consulting & Training

SN	Manpower/ Analyst/ Resource Type	Job Description
		• Communicating Emergency Alerts & Warnings to relevant/ designated stakeholders • Perform analysis on the reported incidents, determine the root cause, recommend the appropriate solution ensure the necessary RSDC SOC documents like operating procedures, configuration management, Low Level Design etc. are up to date with the changes made in their respective areas.
4.	Threat Hunter Regular Day Shift	• Certified with any threat hunting certification, or equivalent • Responsible for conducting all threat-hunting activities necessary for identifying the threats including zero day. • Hunt for security threats, identify threat actor groups and their techniques, tools and processes • Provide expert analytic investigative support to L1 and L2 analysts for complex security incidents. • Perform analysis of security incidents for further enhancement of rules, reports, AI/ML models • Perform analysis of network packet captures, DNS, proxy, NetFlow, malware, host-based security and application logs, as well as logs from various types of security sensors uncovering the unknown about internet threats and threat actors • Analyse logs, alerts, suspicious malwares samples from all the SOC tools, other security tools deployed in the RSDC such as Anti-Virus, EDR, IPS/IDS, Firewalls, Proxies, Active Directory, Vulnerability assessment tools etc. • Using knowledge of the current threat landscape, threat actor techniques, and the internal network, analyze log data to detect active threats within the network. Build, document and maintain a comprehensive model of relevant threats to the RSDC SOC. • Proactively identify potential threat vectors and work with team to improve prevention and detection methods. • Identify and propose automated alerts for new and previously unknown threats. • Incident Response
5.	Risk & Compliance Auditor Regular Day Shift	• Driving SOC audits and managing the day-to-day responsibilities of gathering evidence, scheduling resources, coordinating with control owners and external auditors.

SN	Manpower/ Analyst/ Resource Type	Job Description
		• Analyze potential risks within the SOC and its practices to avoid possible compliance issues. • Review all relevant programs and activities affected by industry regulations, including records, reports, and software. • Recommend and implement changes to address procedures and practices that are not compliant with industry regulations. • Educate, consult, evaluate, and advise internal stakeholders on internal SOX controls and risk mitigation in an ever-changing environment. • Participate on project teams to ensure that enterprise risks and SOX controls are appropriately considered, identified early, and managed proactively in the project development lifecycle. • Identify potential audit issues and operational improvements specific to the SOC 2 audits. • Familiarity with cybersecurity frameworks (i.e., NIST, COSO, COBIT, and/or ITIL etc.) as well as third party assurance reports (SOC 1, 2, 3). • Proficiency in compliance management software and tools.
6.	SOC Manager Regular Day Shift	• Provide the first line supervision to GoR and to Lead and manage the Security Operations Center. • Develop and administer SOC 2 type II processes and review their application to ensure that SOC's controls, policies, and procedures are operating effectively • Primarily responsible for overall security event monitoring, management and response • Ensure incident identification, assessment, quantification, reporting, communication, mitigation and monitoring • Ensure compliance to SLA, process adherence and process improvisation to achieve operational objectives • Revise and develop processes to strengthen the current Security Operations Framework, Review policies and highlight the challenges in managing SLAs. • Responsible for team & vendor management, overall use of resources and initiation of corrective action where required for Security Operations Center

SN	Manpower/ Analyst/ Resource Type	Job Description
		• Management, administration & maintenance of security devices under the purview of GoR which consists of state-of-the art technologies • Perform threat management, threat modeling, identify threat vectors and develop use cases for security monitoring • Creation of reports, dashboards, metrics for SOC operations and presentation to Sr. Mgmt. • Co-ordination with stakeholders, build and maintain positive working relationships with them • Produce and review aggregated performance metrics • Manage and increase the effectiveness and efficiency of the SOC, through improvements to each function as well as coordination and communication between support and business functions • Play a significant role in long-term SOC strategy and planning, including initiatives geared toward operational excellence
	Forensic Analyst	• Respond to and investigate security incidents, breaches, or suspicious activities. This involves identifying the nature and scope of the incident, containing it, and gathering evidence for further analysis. • Collect and preserve digital evidence from various sources, including computers, servers, mobile devices, and network logs. Ensure that the evidence is gathered in a forensically sound manner to maintain its integrity. • Employ specialized tools and techniques to recover data from compromised or damaged systems, with an emphasis on preserving the original data and maintaining a chain of custody. • Create forensic images of digital devices to create an exact copy of their contents. This image is used for analysis while preserving the original evidence. • Maintain a detailed record of the handling and custody of digital evidence to ensure its admissibility in legal proceedings. • Examine digital evidence to identify signs of compromise, unauthorized access, or other security incidents. Collaborate with other teams, such as cybersecurity and legal, to support investigations.

SN	Manpower/ Analyst/ Resource Type	Job Description
		• Document all forensic procedures, findings, and analysis in comprehensive reports. These reports may be used in legal proceedings or for internal reviews. • In some cases, provide expert testimony in legal proceedings to explain findings, methodologies, and the importance of digital evidence. • Offer recommendations and guidance to improve security based on findings from forensic investigations. This may include suggesting security enhancements, policy changes, or staff training.
7.	OEM Certified Resource	• Resource should be Certified on respective OEM technology. • Integrate respective solution / technology with every other solution / technology deployed in the RSDC setup • Automation of all L1 & L2 activities • Collaborate closely with Technical Account Manager (TAM) and engineering division of the respective OEM for early resolution to the product level cases, vulnerabilities, bugs, features enhancement, patches, versions etc. • Single point of contact to the RSDC SOC with respective OEM • Maintain the suitable architecture of the technology solution • Execute Major changes without any disruption and adverse impact • Continuously deliver the value of solution to the RSDC SOC for detecting all kind threats, accuracy of detection, value added use cases and content development etc. • Improvise threat hunting capabilities of the technology • Continuous development of analytical, statistical, mathematical models leveraging AI/ML capabilities of the technology to threat detection and prediction capabilities and put in place advanced use cases • Continuous fine tuning of configuration, rules, policies etc. • Continuous innovation and automations in intuitive dashboards, report, queries • Optimization of response time to fetch data, logs in advanced queries, reports, dashboards etc. • Closely collaborate with onsite team of bidder and other RSDC SOC OEMs to leverage each technology's

SN	Manpower/ Analyst/ Resource Type	Job Description
		capabilities to develop inter-SOC and inter-IT Infrastructure technologies& services, logs, data ingestion, correlation, alerting etc. and automation • Threat Intel feed analysis, provide appropriate recommendations, define use cases to detect the threats according to the information provided in Threat intel • Troubleshooting the technology level issues to ensure uptime, health, efficiency and optimal utilization of the technology support from offsite subject matter experts. • Close the vulnerabilities, apply security & enhancement patches, upgrade versions. • Responsible for ensuring end to end tight integration of the RSDC other SOC solutions, Applications etc. • Provide management report on respective solutions effectiveness • Provide necessary support during the Forensics investigation and threat hunting • Perform continuous assessment of respective solution maturity against global standards and fine tune the configuration parameters, technical policies, rules, algorithms accordingly. • Prepare road map for product maturity and enhancements plan and ensure the recommended featured deliver within the agreed times. • Participate in meetings, discussions etc. to provide technology specific perspective. Make presentations on the current technology capabilities, use cases, automation done etc. and current and future enhancements / roadmap etc.